512.73
E91u

Burg

THE UNIVERSITY
OF ILLINOIS
LIBRARY
512.8~~13~~ 73
B91u
MATHEMATICS
DEPARTMENT

Über die

Eulerschen und Gaußschen Methoden der Primzahlbestimmung.

Inaugural-Dissertation

der

hohen mathematischen und naturwissenschaftlichen Fakultät

der

Kaiser-Wilhelms-Universität Straßburg

zur

Erlangung der Doktorwürde

vorgelegt von

RICHARD BURGWEDEL

aus Straßburg (Elsaß).

Straßburg i. E.

Druck von M. DuMont Schauberg.

1910.

LIBRARY
UNIVERSITY OF ILLINOIS
URBANA

512.813 73
B91u

UNIVERSITY OF ILLINOIS LIBRARY URBANA

INHALT.

Einleitung: Bemerkungen zur Geschichte des Primzahltheorems.

I. Eulers Methoden der Primzahlbestimmung.

Kurze Charakteristik derselben; ihr gemeinschaftliches Prinzip ein Subtraktionsverfahren

$$M - ax^2 = cy^2.$$

Die 2 Hauptfragen Eulers: Welche Formen und welche Zahlen eignen sich zur Untersuchung?

Kurze Zusammenfassung der Theorie der quadratischen Form (a, b, c) (b = o) und derjenigen der Formen einer gegebenen Determinante D.

Einfachste negative Determinanten D = — 1, — 2, — 3, — 5.

Sätze Eulers über die Form (a, o, c).

Die beiden Eulerschen Hauptmethoden. — Ihre theoretische Grundlage. Sie benützen zur Primzahlbestimmung die Formen (1, 0, 1) und (1, 0, 2). Diese zerlegen jede zusammengesetzte Zahl, wenn dies überhaupt geschieht, mehrmals; eine Primzahl dagegen, wie alle andern quadratischen Formen, nur einmalig. Somit sind (1, 0, 1) und (1, 0, 2) geeignete Formen (formae congruae vel idoneae).

Darstellung der Methode an 3 Beispielen. — Ihre Erweiterung auf die Form (1, 0, 5).

Ermittlung der kongruenten Formen (a, o, c). In der Ausdrucksweise der Gaußschen Theorie sind es alle diejenigen, in denen — ac eine der 65 in ihren eigentlich primitiven Geschlechtern einklassigen Determinanten D_1 darstellt. Euler bezeichnet diese 65 D_1 als kongruente Zahlen (numeri idonei vel congrui). Er entnimmt sie folgendem Kriterium: Bleiben die Summen $x^2 + \Delta$ im Intervalle Δ bis 4 Δ, wo x und Δ ganz und relativ prim, prim oder primäquivalent, dann ist Δ eine kongruente Zahl; wird aber nur eine zusammengesetzt, so ist Δ inkongruent. Primäquivalent sind die Doppelwerte der Primzahlen und sämtliche Potenzen der 2.

264819

Eulers Beweise zu seinem Kriterium unzulänglich. Beweis durch die Gaußsche Theorie für die 65 D_1.

Eulers Sätze über die kongruenten Formen.

Seine Subtraktionsmethode in Anwendung auf jede beliebige kongruente Form (a, o, c), ($ac = -D_1 = \Delta_1$). Da die zugehörigen Linearformen (die Gaußschen Teilerformen von $D_1 = -ac$) fehlen, bleibt die 2. Hauptfrage offen. Die kongruenten Formen werden der Reihe nach herangezogen, bis eine unter ihnen eine Zerlegung der zu untersuchenden Zahl M gibt. Geht aus der Fortsetzung der Untersuchung eine zweite, von der ersten verschiedene Zerlegung von M hervor, so zeigt diese ein zusammengesetztes M an, dessen Primteiler nach dem in Eulers Sätzen über die Form (a, o, c) niedergelegten Algorithmus sich ergeben. Im entgegengesetzten Falle bekundet sich M als prim.

Darstellung der Methode und ihrer Vereinfachung durch Substitutionen an 3 Beispielen.

Schlußbemerkung zu Euler.

II. Die beiden Gaußschen Methoden der Primzahlermittlung.

Die Gaußsche Einleitung zu seinen Methoden

1. Methode

eine Anwendung der Theorie der quadratischen Reste.

Ihr Hilfssatz: Jeder quadratische Rest von M ist auch quadratischer Rest von jedem Teiler von M.

Ihr Prinzip: Aufstellung des Primzahlkomplexes $\Omega < \sqrt{M}$ und Zurückführung desselben auf die Primteiler von M. Alle diejenigen Primzahlen werden nämlich aus Ω ausgeschlossen, die einen quadratischen Rest von M zum Nichtrest haben. Diese Ausschließung bewirkt Tafel I, die die quadratischen Charaktere der Zahlen von — 100 bis + 100 bezüglich aller Primteiler von 1 — 1000 enthält[1]). Hat man Reste von M in jenem Intervalle gefunden und legt die diesen entsprechenden Vertikalspalten nebeneinander, so sind meistens diejenigen Primzahlen Teiler von M, deren Horizontalspalte kein leeres Feld enthält. Zur Ermittlung tauglicher Reste von M drei Wege, dazu Verallgemeinerung des ersten in einem vierten.

[1]) Ein Horizontalstrich gibt den Restcharakter, die Abwesenheit jeglichen Zeichens den entgegengesetzten Charakter an.

a) Zerlegung von M in 2 Summanden: $M = a + b$; dann — ab R M.

b) Entwicklung der Periode der Hauptklasse der positiven Determinante + M oder + k · M. Die Periodenformen gehören in dieselbe Klasse und mithin in dasselbe Geschlecht. Dann ist aber das Produkt aus einer geraden Anzahl ihrer Außenglieder stets Rest von M.

c) Bildung der Periode einer Form (a, b, c) der negativen Determinante — M oder — k · M. Gehört (a, b, c) in die Klasse C, so entfallen die Klassen mit ungeradem Exponenten $C^1, C^3, C^5 \ldots C^{2m+1}$ auf das Geschlecht G von C, dagegen die Klassen $C^2, C^4, C^6 \ldots C^{2m}$ auf das Hauptgeschlecht G_H. In G sind die Produkte aus einer geraden Zahl von Außengliedern, in G_H diese selbst Reste von M. Algorithmus der Zusammensetzung; seine theoretische Begründung und seine Vereinfachung für den Fall $a = 3$ und $k \cdot M \equiv 2 \pmod 3$, der durch geeignete Wahl von k stets erreicht wird.

d) Ermittlung von Formen, die M eigentlich darstellen und deren Determinante D mithin allemal Rest von M ist.

Gesamtdarstellung der 1. Methode an 3 Beispielen.

2. Methode

im Kerne eine Anwendung der Theorie der quadratischen Formen.

Sie nimmt ihren Ausgang von folgendem Satz:

Hat die Kongruenz

$$(A)\ x^2 \equiv D \pmod M,$$

wo M prim zu 2 D vorausgesetzt ist, nur 2 entgegengesetzte Wurzeln, so ist M prim oder primäquivalent (die Potenz einer Primzahl oder das Doppelte einer solchen). Befriedigen sie aber 2μ paarweis entgegengesetzte Wurzeln, so ist M aus μ verschiedenen, ungeraden Primteilern zusammengesetzt.

Ermittelung der Wurzelzahl von (A).

Die Wurzeln von (A) gehören zu den eigentlichen Darstellungen von M durch die Formen des eigentlich primitiven Geschlechts G von D, dessen Totalcharakter M trägt. Ein primes M muß durch G zur Darstellung kommen, ein zusammengesetztes nur dann, falls keiner seiner Primteiler D zum Nichtrest hat. Wird M überhaupt nicht dargestellt, so enthält M eine gerade Zahl Primteiler mit dem Nichtreste D.

Man bestimmt also sämtliche Darstellungen von M durch die repräsentierenden Formen von G. Sind α und γ die Unbestimmten einer solchen, so genügt die zugehörige Wurzel den beiden Kongruenzen:

$$a\alpha + b\gamma + n\gamma \equiv b\alpha + c\gamma - n\alpha \equiv o \pmod{M}.$$

Summe und Differenz je eines Paares inkongruenter Wurzeln von (A) enthalten zusammen sämtliche Primfaktoren von M. Die 65 einklassigen Determinanten D_1 führen, da sie nur die Untersuchung einer einzigen Form verlangen, offenbar am schnellsten zum Ziele.

Ausdehnung der Methode auf mehrklassige Determinanten. Um auch für solche die Untersuchung nur auf eine Form zu beschränken, transformiert man die repräsentierenden Formen von G

$$(\mu_1, \nu_1, \pi_1) \quad (\mu_2, \nu_2, \pi_2) \quad \ldots\ldots \quad (\mu_n, \nu_n, \pi_n)$$

durch Multiplikation mit m, wo m die kleinste durch sämtliche von ihnen eigentlich oder uneigentlich dargestellte Zahl vorstellt, auf die Hauptform (1, o, Δ) oder die ambige Form $\left(\delta, o, \frac{\Delta}{\delta}\right)$ von D. Ersetzt man eine uneigentliche Darstellung von $m \cdot M$ oder $m' \cdot M$ durch eine eigentliche von $\mu \cdot M$, bzw. $\mu' \cdot M$, so finden Darstellungen von $m \cdot M$ oder $m' \cdot M$ zu allen Wurzeln von (A) gehörig statt.

Ergibt sich deren bloß eine einzige, so ist M sicherlich prim. Aus einer Mehrzahl von ihnen leitet man etwaige Primfaktoren von M nach dem oben erwähnten Algorithmus ab.

Einrichtung der Tafel II.

Sie ordnet einzelnen Geschlechtern von 296 Determinanten die Hülfszahlen m zu.

Durchführung der 2. Methode an 4 Beispielen.

Schluß: Gegenüberstellung von Euler und Gauß.

Über die Eulerschen und Gaußschen Methoden der Primzahlbestimmung.

Unter die Probleme, welche schon seit den ersten Anfängen der mathematischen Wissenschaften im Brennpunkt des Interesses standen, gehört auch dasjenige, den primen oder zusammengesetzten Charakter einer gegebenen Zahl zu bestimmen. Wie in der Geometrie die Quadratur und Rektifikation des Kreises, so hat in der Arithmetik jenes Problem die führenden Geister schon seit Euklids Zeiten beschäftigt. Euklid war es bekanntlich, der die unendliche Menge der Primzahlen erkannte. Nach dem Ausgange des fortschrittlosen Mittelalters erwachte wie jede andere Wissenschaft auch die Mathematik zu neuer Blüte, und auf zahlentheoretischem Gebiete ragte unter allen andern der scharfsinnige Fermat hervor. Er erweiterte und vertiefte zunächst die Arithmetik Diophants, d. h. die Lehre von den unbestimmten Gleichungen; dann wandte er sich rein zahlentheoretischen Untersuchungen zu und entdeckte hierbei eine Reihe schöner und eleganter Sätze, wie unter andern den erst von Euler bewiesenen (vgl. S. 14), daß jede Primzahl von der Form $4n + 1$ als Summe von 2 Quadraten darstellbar ist. Da er manche seiner Sätze ohne Beweis veröffentlichte, dessen eigene Kenntnis er jedoch versicherte, so hatte die mathematische Forschung neue Kristallisationspunkte gewonnen. Ein Jahrhundert später wandte sich der ungemein vielseitig arbeitende Euler ihrer Begründung zu. Vor allem fesselte ihn die Fermatsche Forderung, von einer gegebenen Primzahl aus die nächstgrößere zubestimmen oder überhaupt eine Gesetzmäßigkeit in der Reihe der Primzahlen aufzuzeigen. Fermat hatte behauptet, daß der Ausdruck

$$2^{2^m} + 1$$

für sämtliche ganzzahligen Werte von m Primzahlen darstelle. Während dies für $m = 0, 1, 2, 3, 4$ zutrifft, weist Euler nach, daß für $m = 5$ $2^{2^5} + 1 = 4\ 294\ 967\ 297$ durch 641 teilbar

wird. Die beschränkte Gültigkeit dieses Gesetzes läßt vermuten, daß Fermat diejenigen Sätze, deren Beweis er weder selber führte, noch führen zu können behauptete, nur auf induktive Gewißheit gründete. Euler zeigt ferner, daß keine ganze algebraische Funktion

$$F(x) = a_0 x^m + a_1 x^{m-1} + a_2 x^{m-2} + \ldots\ldots + a_m$$

für sämtliche Werte der Unbestimmten x Primzahlen liefert. Denn wird sie für $x = x_0$ prim, so wird sie für alle Werte

$$x \equiv x_0 \pmod{F(x_0)}$$ durch $F(x_0)$ teilbar.

Trotz seiner Bemühungen gelingt es ihm nicht, jenes Problemes Herr zu werden; er vergleicht die Schwierigkeit seiner Lösung mit der der Quadratur des Kreises. Muß er auch darauf verzichten, durch Angabe funktionaler Beziehungen Primzahlen zu bilden, da diese Aufgabe genau wie die ihr gegenübergestellte geometrische wohl an strenger Unausführbarkeit scheitert, so hat er doch verschiedene Methoden geschaffen, zu entscheiden, ob eine gegebene, nicht zu große Zahl prim ist oder nicht. Zunächst dient dazu das nach ihm benannte Eulersche Kriterium, das aber allgemein praktischer Brauchbarkeit ermangelt, obwohl es im besonderen Falle Euler die Teilbarkeit von $2^{2^5} + 1$ verriet. Bezeichnen nämlich p eine Primzahl und n eine beliebige Zahl, in der p nicht aufgeht, so bestehen nur für prime Module die Kongruenzen:

$$n^{\frac{p-1}{2}} \equiv +1 \text{ oder } \equiv -1 \pmod{p},$$

je nachdem n quadratischer Rest oder Nichtrest von p ist. Die Methoden, welche er zu allgemeiner Brauchbarkeit erhoben hat, verfolgen alle dasselbe Prinzip; nämlich die gegebene Zahl als Summe von zwei einfach oder mehrfach genommenen Quadraten darzustellen, worauf gleich unten eingegangen werden wird. Obwohl sie die früheren an Kürze der Rechnung übertreffen, verlieren sie doch ihren praktischen Nutzen, sobald die zu untersuchenden Zahlen im allgemeinen den Zahlenkreis von 1—1 000 000 verlassen. Seinem größeren Nachfolger Gauß, dem Begründer einer in sich abgeschlossenen Zahlentheorie, war es vergönnt, Methoden darzubieten, die ihren praktischen Wert auch noch bei achtstelligen Zahlen bewahren. Ihm stand das ganze Rüstzeug der durch ihn erstandenen Wissenschaft, der Lehre von den Kongruenzen, den quadratischen Resten und

Formen zu Gebote, und als eine Anwendung derselben treten uns seine Methoden, die allerdings auch noch innerhalb des gewöhnlich durchlaufenen Zahlengebietes ihre Grenze erreichen, entgegen. Das Ziel vorliegender Arbeit soll es nun sein, die Methoden beider Männer darzulegen und verschiedentlich zu erweitern.

Voreulersche Mittel der Primzahlbestimmung.

Bevor wir uns den Eulerschen Untersuchungen zuwenden, berühren wir kurz die zuvor bekannten Mittel, Primzahlen zu bestimmen. Der Wilsonsche Satz bot dazu zunächst eine Möglichkeit. Bezeichnet p eine Primzahl, so ist das um 1 vermehrte Produkt aller p vorhergehenden Zahlen durch p teilbar, d. h.

$$1.\,2.\,3.\,4\,\ldots\ldots,\,.\,(p-1) \equiv -1 \pmod{p}.$$

Wäre p zusammengesetzt, so müßte die linke und damit auch die rechte Seite dieser Kongruenz durch jeden Faktor von p teilbar sein, was ungereimt ist. Da mithin dem Satze nur Primzahlen genügen, gewährt er für diese ein Erkennungszeichen, das jedoch in der Praxis völlig versagt. Ein anderer Weg (vgl. Legendre, Théorie des nombres I S. 5) hält sich an folgende Erwägung. Ist M zusammengesetzt, so kann nur ein Primteiler von $M > \sqrt{M}$ sein, während die übrigen $< \sqrt{M}$ sein müssen. Ist somit die Division von M durch alle Primzahlen $< \sqrt{M}$ vergeblich, so ist M sicher prim. Jedoch wirkt auch diese Methode, die übrigens die Kenntnis der unter $\sqrt{M}$ liegenden Primzahlen voraussetzt, bald ermüdend und wird, wenn M in die Hunderttausende rückt, wohl aufgegeben werden.

Die beiden Hauptfragen der Eulerschen Untersuchung.

Als ihre erhebliche Verbesserung wertet Euler seine eigenen Methoden. Diese sind in den Commentationes arithmeticae enthalten, die von der Petersburger Akademie der Wissenschaften in 2 Bände gesammelt worden sind, und zwar in den Abhandlungen 12, 13, 25, 26 des 1. Bandes (C 1, 12; 1, 13; 1, 25; 1, 26) und 59—63 des 2. Bandes (C 2, 59—63).

In ihnen behandelt er Formen von der Gestalt

$$ax^2 + cy^2,$$

in denen a u. c ganzzahlige, positive Koeffizienten, x u. y Un-

bestimmte vorstellen. Außer den allgemeinen Eigenschaften dieser Formen treten 2 Fragen in den Vordergrund: 1) Zahlen welcher linearer Formen werden durch eine gegebene quadratische $ax^2 + cy^2$ dargestellt? 2) Wieviel Mal werden diese Zahlen durch $ax^2 + cy^2$ dargestellt? Die Beantwortung der 1. Frage entscheidet, ob sich die gegebene Zahl, die der zweiten, ob sich die gegebene Form zur Untersuchung eignet. Alle diejenigen Formen werden nämlich von ihr ausgeschlossen, die irgend welche zusammengesetzte Zahlen nur einmal zur Darstellung bringen. Stellen dann die übrigbleibenden Formen eine Zahl nur einmalig dar, so muß diese notwendig prim sein. Umgekehrt kann, wie allgemein gilt, keine Primzahl mehrmals in der gleichen Form enthalten sein. Denn wäre, wo p prim:

$$\begin{array}{l} p = ax_1^2 + cy_1^2 \mid x_2y_2 \\ p = ax_2^2 + cy_2^2 \mid x_1y_1 \end{array},$$

so würde daraus folgen:

$$p\,(x_1y_1 - x_2y_2) = (ax_1x_2 - cy_1y_2)\cdot(x_2y_1 - x_1y_2)$$

p ist aber größer als jeder der beiden Faktoren der rechten Seite, kann also nicht prim sein. Euler erschließt dann die Anzahl aller möglichen Darstellungen von M durch eine Kette von Subtraktionen. Er zieht nämlich von M den einen Summanden mit steigenden oder fallenden Werten seiner Unbestimmten ab und sieht nach, ob die Differenz die Form des 2. Summanden annimmt, wobei die Rechnung durch allerlei Kunstgriffe erheblich zusammengezogen wird. Der näheren Entwicklung seiner Algorithmen soll aber erst eine Zusammenfassung dessen vorangehen, was vom Standpunkte der heutigen Lehre von den quadratischen Formen über jene beiden Hauptfragen geurteilt werden kann.

Zusammenfassung der Theorie der Form (a, b, c).

a) Darstellung einer Zahl M durch (a, b, c).

Stellt die gegebene quadratische Form (a, b, c) eine Zahl M dar, sodaß

$$(1)\quad ax^2 + 2b\,x\,y + cy^2 = M,$$

so werden x u. y entweder zu einander prim sein oder einen von 1 verschiedenen größten gemeinschaftlichen Teiler δ besitzen. Im ersteren Falle nennt man die Darstellung eigentlich, im letzteren uneigentlich. Für die erstere ist bekanntlich die

notwendige, aber nicht ausreichende Bedingung, daß die Determinante $D = b^2 - ac$ der Form (a, b, c) quadratischer Rest von M ist: D R M. Genügen der Kongruenz

$$(A)\quad x^2 \equiv D \pmod{M}$$

die Wurzeln $+n_1, -n_1, +n_2, -n_2, +n_3, -n_3 \ldots . +n_m, -n_m$, so ordnet sich jedem n eine Gruppe eigentlicher Darstellungen zu, deren Unbestimmte x, y allemal mit n durch die Gleichung verbunden sind:

$$(ax + by)\,\beta + (bx + cy)\,\delta = n,$$

wo β u. δ so bestimmt sind, daß

$$x \cdot \delta - y \cdot \beta = 1,$$

oder durch die linearen Kongruenzen:

$$\begin{aligned} ax + by + ny &\equiv o \\ bx + cy - nx &\equiv o \end{aligned} \pmod{M};$$

Kennt man aus der Gruppe eine Darstellung (α, γ), so folgen die übrigen aus der Gleichung:

$$(2)\quad ax + by + y\sqrt{D} = (a\alpha + b\gamma + \gamma\sqrt{D})\,(t + u\sqrt{D}),$$

wo t u. u die Auflösungen der Pell'schen Gleichung

$$t^2 - Du^2 = 1$$

bedeuten, deren Anzahl mithin diejenige der Darstellungen in der Gruppe bestimmt. Hierüber entscheidet das Vorzeichen von D.

I. $D > o$

Da positive Determinanten in den folgenden Untersuchungen nirgends unterlaufen, fällt die Betrachtung des Falles I fort.

II. $D < o$; $D = -\Delta$; $\Delta < o$

Mit Rücksicht auf den Zweck dieser Vorbemerkungen werden 2 Unterfälle auseinandergehalten.

1. $b = o$

Für $D < o$ läßt die Pell'sche Gleichung i. A. nur noch 2 Lösungen zu, nämlich $t = \pm 1$, $u = o$. Eine Ausnahme bildet der Fall $D = -1$, für den sich ihre Zahl verdoppelt: $t = \pm 1$, $u = o$; $t = o$, $u = \pm 1$. I. A. umfaßt also die zu einer Wurzel n gehörige Darstellungsgruppe nur noch 2 Darstellungen: $ax + by + y\sqrt{D} = (a\alpha + b\gamma + \gamma\sqrt{D})\,(\pm 1)$, deren Unbestimmte offensichtlich einander entgegengesetzt sind. Solche 2 Darstellungen geben nur eine Zerlegung von M in Vielfache von zwei Quadraten und deren doppeltem Wurzelprodukt;

deshalb werden sie für die Folge nicht mehr voneinander geschieden. Ist M prim, so befriedigen die Kongruenz (A) 2 entgegengesetzte Wurzeln + n u. — n. Mithin kann M zweifach in (a, b, c) eingehen. Umgekehrt ist M zusammengesetzt und hat somit (A) i. A. mehrere Paare entgegengesetzter Wurzeln, so kommt es vor, daß trotzdem nur zu einer von ihnen eine Darstellung erfolgt, M mithin nur auf eine einzige Art in (a, b, c) enthalten ist. Im Falle $D = -1$ wird aus Gl. (2):

$$ax + by + y\sqrt{-1} = (a\alpha + b\gamma + \gamma\sqrt{-1}) \begin{pmatrix} \pm 1, & o \\ o, & \pm\sqrt{-1} \end{pmatrix},$$

woraus die 4 Darstellungen hervorgehen:

$x_1 = \alpha$; $x_2 = -\alpha$; $x_3 = b\alpha + c\gamma$; $x_4 = -(b\alpha + c\gamma)$
$y_1 = \gamma$; $y_2 = -\gamma$; $y_3 = -(a\alpha + b\gamma)$; $y_4 = +(a\alpha + b\gamma)$

Da sie paarweise entgegengesetzt sind, fallen somit auf jede Wurzel 2 Zerlegungen. Eine Primzahl nimmt also möglicherweise vierfach eine Form mit der Determinante -1 und nichtverschwindendem Mittelgliede an.

2. $b = o$

Die quadratische Form $ax^2 + cy^2$ deckt sich nun mit der Eulerschen, weswegen ihr eine besondere Stellung gebührt. Ihre Determinante $D = -ac$ ist negativ; (2) erscheint in der einfacheren Gestalt:

$$ax + y\sqrt{D} = (a\alpha + \gamma\sqrt{D}) \cdot (\pm 1)$$

Während wiederum mit einer Wurzel n von (A) eine Zerlegung von M verbunden ist, tritt doch insofern eine Verminderung ihrer Gesamtzahl ein, als sich die auf ein Paar entgegengesetzter Wurzeln von (A) entfallenden Darstellungen von M nur durch das Vorzeichen unterscheiden. In der Tat erfüllen α, γ u. $-\alpha$, $-\gamma$ die Kongruenzen:

$$a\alpha + n\gamma \equiv o \quad c\gamma - n\alpha \equiv o \pmod{M},$$

so genügen α, $-\gamma$ u. $-\alpha$, γ diesen Kongruenzen mit entgegengesetzter Wurzel $-n$:

$$a\alpha' - n\gamma' \equiv o \quad c\alpha' + n\gamma' \equiv o \pmod{M}$$

und gleichzeitig der gegebenen Gleichung $ax^2 + cy^2 = M$. Einem Paar entgegengesetzter Wurzeln von (A) entspricht demnach nur eine Zerlegung von M durch (a, o, c) oder in ein a-faches und c-faches Quadrat. Hieraus folgt, daß Primzahlen nur einer einzigen solchen Zerlegung fähig sind oder nur einmal in (a, o, c) enthalten sein können. Ist im besondern Falle

(a, o, c) = (1, o, 1) oder D = −1, so ordnen sich der Wurzel n von (A) die 4 Darstellungen zu:

$$\alpha;\quad -\alpha;\quad \gamma;\quad -\gamma$$
$$\gamma;\quad -\gamma;\quad -\alpha;\quad +\alpha$$

der entgegengesetzten — n folgende 4:

$$\alpha,\ -\alpha,\ \gamma,\ -\gamma$$
$$-\gamma,\quad \gamma,\ \alpha,\ -\alpha$$

Auf ein Paar entgegengesetzter Wurzeln entfällt mithin nur eine Zerlegung von M in 2 Quadrate. Ein primes M kann also nur einmal gleich der Summe zweier Quadratzahlen werden.

b) Darstellung von M durch die Formen von D.

Alle quadratischen Formen, die in ihrer Determinante D übereinstimmen, bilden den Formenkomplex von D. Er zerfällt zunächst in Klassen; eine Klasse vereinigt alle diejenigen Formen, die dieselben Zahlen zu denselben Wurzeln von (A) gehörig darstellen, die also einander äquivalent (nach Gauß eigentlich äquivalent) sind. Jede Klasse paart sich mit einer entgegengesetzten; dieser gehört die entgegengesetzte Form zu jeder Form von jener an. Beide stellen die gleichen Zahlen, aber zu entgegengesetzten Wurzeln von (A) gehörig dar. Klassen, welche sich selbst entgegengesetzt sind, heißen ambig (classes ancipites nach Gauß).

1. M prim oder primäquivalent

(beliebige Primzahlpotenz oder das Doppelte einer solchen).

(A) hat dann nur ein Paar entgegengesetzter Wurzeln. Folglich können sich an der Darstellung von M nur 2 entgegengesetzte oder eine ambige Klasse beteiligen.

2. M zusammengesetzt

aus μ unter sich und von denen der Determinante verschiedenen ungeraden Primfaktoren, welche Zusammensetzung die vorliegende Untersuchung stets antreffen wird. (A) besitzt 2^{μ} (mod. M) inkongruente Wurzeln, die paarweise einander entgegengesetzt sind. Dadurch sind zwei 2^{μ} Formen bestimmt, welche M zur Darstellung bringen, nämlich

$$(M, +n_1, m_1) \qquad (M, -n_1, m_1)$$
$$(M, +n_2, m_2) \qquad (M, -n_2, m_2)$$
$$(M, +n_3, m_3) \qquad (M, -n_3, m_3)$$
$$\vdots \qquad\qquad \vdots$$
$$(M, +n_m, m_m) \qquad (M, -n_m, m_m),$$

wo allgemein $m = \frac{n^2 - D}{M}$ gesetzt ist. Sie können sich auf eine oder auf mehrere Klassen verteilen, hierin waltet keine Gesetzmäßigkeit. M kann folglich bloß durch eine, dann durch mehrere, schließlich sogar durch alle Klassen dargestellt werden.

3. Die einfachsten negativen Determinanten.

Besondere Stellung verdienen die einfachsten negativen Determinanten, nicht allein aus rein zahlentheoretischen Gesichtspunkten, sondern auch schon deshalb, weil sie denjenigen Formen Eulers zukommen, auf die er seine Hauptmethoden anwendet.

Da für die Determinanten — 1 und — 2 nur je eine reduzierte Form besteht (vgl. D. A. Art. 171), nämlich (1, 0, 1) bzw. (1, 0, 2) so sind es die einzigen, deren Formen nur je eine Klasse füllen.

α) $D = -1$.

Jede Zahl M_{-1} mit dem quadratischen Reste — 1 erfährt somit Darstellungen durch sämtliche Formen von $D = -1$. M_{-1} hat notwendig die lineare Form $4n + 1$. Denn setzt man in der Formel des Eulerschen Kriteriums: $n^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ $n = -1$, so hat das obere oder das untere Vorzeichen statt, je nachdem p von der Form $4n + 1$ oder $4n + 3$ ist. Da mithin — 1 Rest aller Primzahlen der ersten Art, dagegen Nichtrest aller derer der zweiten Art ist, so kann sich M_{-1} nur aus solchen der ersten Art zusammensetzen, was M_{-1} in die behauptete Form bringt. Finden sich unter jenen μ verschiedene ungerade, so gelangt M_{-1} durch jede Form der Determinante — 1 außer (1, 0, 1) $2^{\mu+1}$mal, durch (1, 0, 1) sogar $2^{\mu+2}$mal zur Darstellung. Stets finden aber $2^{\mu-1}$, also gleich viel Zerlegungen durch alle Formen statt (vgl. S. 13). Ist M_{-1} prim, so ist für ein solches M $\mu = 1$; man gewinnt den Fermatschen Satz: Jede Primzahl von der Form $4n + 1$ läßt sich und zwar nur auf eine einzige Weise in 2 Quadrate zerlegen.

β) $D = -2$.

Jede Zahl M_{-2} mit dem Reste — 2 wird durch sämtliche Formen mit der Determinante — 2 dargestellt und zwar doppelt soviel Mal, als der Kongruenz $x^2 \equiv -2 \pmod{M_{-2}}$ Wurzeln genügen. Gauß beweißt (D. A. Art. 112—116) daß — 2 Rest aller Primzahlen von den Formen $8n + 1$ oder $8n + 3$ ist; nur

aus solchen kann M_{-2} gebildet sein. Sind es ihrer Zahl nach μ, so findet eine $2^{\mu-1}$fache Zerlegung von M_{-2} in ein einfaches und doppeltes Quadrat durch den gesamten Formenkomplex von $D = -2$ statt. Ist insbesondere $\mu = 1$, so folgt der zuerst von Lagrange bewiesene Satz: Jede Primzahl von der Form $8n + 1$ oder $8n + 3$ kommt ein einziges Mal durch Addition eines einfachen und doppelten Quadrates zustande.

γ) $D = -3$.

Für $D = -3$ ergeben sich 2 reduzierte Formen: (1, 0, 3) und (2, 1, 2). Es zerfallen mithin sämtliche Formen mit der Determinante -3 in **2** Klassen, in eine eigentlich primitive, die durch die erste, und in eine uneigentlich primitive, die durch die zweite reduzierte Form vertreten wird. Da eine Klasse letzter Art nur gerade Zahlen darstellen kann, müssen somit alle ungeraden Zahlen M_{-3} mit dem Reste -3 durch die eigentlich primitive Klasse und somit auch durch (1, 0, 3) zur Darstellung kommen. Da, wie das Reziprozitätsgesetz lehrt, -3 Rest aller Primzahlen von der Form $3n + 1$ ist, eine Primzahl aber allgemein nur eine Zerlegung durch (a, o, c) gestattet, so ergibt sich der von Euler (C 1, 21) entdeckte und bewiesene Satz: Jede Primzahl der Form $3n + 1$ zerlegt sich einmalig in ein einfaches und dreifaches Quadrat. Jedes zusammengesetzte M_{-3} kann es offenbar nur aus solchen Primteilern sein.

Da jeder Faktor einer Zahl mit dieser in den Resten übereinstimmt, so muß jeder Teiler von M_{-1}, M_{-2}, M_{-3} bzw. durch (1, 0, 1), (1, 0, 2) und (1, 0, 3) zerlegt werden oder ebenfalls bezw. die Formen annehmen $x^2 + y^2$, $x^2 + 2y^2$, $x^2 + 3y^2$.

δ) $D = -5$.

Zu $D = -5$ gehören die beiden reduzierten, eigentlich primitiven Formen (1, 0, 5) und (2, 1, 3). Sämtliche Formen mit der Determinante -5 verteilen sich demgemäß auf 2 eigentlich primitive Klassen, welche für sich je ein Geschlecht bilden. Das erste mit der einfachsten Form (1, 0, 5) hat den Totalcharakter R 5, das zweite mit (2, 1, 3) als einfachster Form N 5. Auf Grund des Reziprozitätsgesetzes ist $+5$ Rest aller Primzahlen von den Formen $5n + 1, 4$. Da -1 Rest solcher von der Form $4n + 1$ ist, muß -5 Rest aller derer von den Formen $20n + 1, 9, 3, 7$ sein. Da die ersten beiden Arten

Rest, die letzten beiden Nichtrest von 5 sind, so werden jene durch das erste, diese durch das zweite Geschlecht dargestellt. Somit folgt: Jede Primzahl von der Form $20n + 1$ oder $20n + 9$ unterwirft sich einer einmaligen Zerlegung in ein einfaches und fünffaches Quadrat. Ferner muß auch jede zusammengesetzte Zahl M_{-5}, die durch das Hauptgeschlecht von $D = -5$ dargestellt wird, in einer der Formen $20n + 1, 9$ enthalten sein. Denn wäre sie es in einer der beiden andern, so müßte dies gleichzeitig von mindestens einem ihrer Primteiler, i. A. aber von einer ungeraden Zahl derselben gelten, was M_{-5} entgegen der Festsetzung zum Nichtrest von 5 machen würde. Da aber einer geraden Anzahl Primteiler von M_{-5} offenbar eine der Formen $20n + 3, 7$ freisteht, so weicht die Determinante $D = -5$ von den vorigen darin ab, daß die Primteiler einer zusammengesetzten Zahl M_{-5} in gerader Menge nicht mit M_{-5} die quadratische Form $x^2 + 5y^2$ zu teilen brauchen, sondern sich der andern $2x^2 + 2xy + 3 \cdot y^2$ erschließen können. Alle 4 besonderen Formen (1, 0, 1) (1, 0, 2) (1, 0, 3) und (1, 0, 5) stimmen aber darin überein, worin sie sich von den allgemeinen (a, o, c) unterscheiden, daß sie jede zu 2 D prime Zahl M, die überhaupt in sie eingeht, halb soviel Mal zerlegen müssen, als M der Kongruenz (A) Wurzeln erteilt. μ verschiedene Primteiler von M bedingen also eine $2^{\mu-1}$fache Zerlegung von M durch eine jener 4 Formen. Ein primes M wird also nur einmalig, dagegen ein zusammengesetztes M mindestens zweimalig zerlegt. Diese Eigenschaft überträgt sich ersichtlicherweise auf alle übrigen eigentlich primitiven Formen der 4 Determinanten; sie kommt allgemein, worauf auf S. 48 noch einmal zurückgegriffen werden wird, allen der 65 einklassigen D_1 zu.

4. Gesamtzahl A aller eigentlichen und uneigentlichen Zerlegungen einer zu $2D_1$ primen Zahl M durch jede eigentlich primitive Form von D_1.

Fällt aus einer zu 2 D primen Zahl M, die D zum Rest hat, wo D vorerst noch eine der vorigen Determinanten darstellt, ein quadratischer Teiler heraus, so wird der Quotient M′, da er entweder die Linearform von M bezüglich D behält oder im Falle $D = -5$ in die mit dieser verbundene über-

geht, gleichfalls durch K zerlegt werden, und zwar $2^{\mu-1}$mal, falls er noch die μ-Primteiler von M enthält, oder $2^{\mu-i}$mal, falls sich ihre Zahl um $(i-1)$ verringert hat. Aus jeder eigentlichen Zerlegung von $M' = \frac{M}{P^2}$

$$M' = ax'^2 + cy'^2$$

folgt aber eine uneigentliche von M:

$$M = P^2 \cdot M' = a(x' \cdot P)^2 + c(y' \cdot P)^2.$$

Diese Eigenschaft, durch ein und dieselbe Klasse M samt den Quotienten aus M und seinen quadratischen Teilern darzustellen, teilen jene 4 Determinanten mit den übrigen 61, die in ihren eigentlich primitiven Geschlechtern nur je eine Klasse enthalten (vgl. S. 48). Da nämlich alle Quotienten M' den Totalcharakter von M bezüglich einer M darstellenden Determinante D_1 bewahren, so müssen sie mit M durch dasselbe Geschlecht und somit durch dieselbe Klasse K zu allen Wurzeln der Kongruenz $x^2 \equiv D_1 \pmod{M'}$ gehörig zerlegt werden. Jede Form aus K führt demnach $2^{\mu-1}$ eigentliche Zerlegungen von M und $2^{\mu-i}$ ebensolche jedes Quotienten M' aus, der $(i-1)$ von den μ Primteilern von M verloren hat. Sie bietet mithin sämtliche eigentlichen und uneigentlichen Zerlegungen von M durch D_1. Zwecks Bestimmung ihrer Gesamtmenge A setzt man M in folgender Gestalt an:

$$M = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot q_3^{\alpha_3} \ldots\ldots q_\nu^{\alpha_\nu} \cdot r_{\nu+1}^{\beta_{\nu+1}} \cdot r_{\nu+2}^{\beta_{\nu+2}} \ldots\ldots r_\mu^{\beta_\mu}$$

wo die α ungerade, die β gerade Exponenten bedeuten. Zunächst erhellt, daß keiner der Exponenten α, dagegen alle β verschwinden können, ferner daß es

$$Bo = \frac{\alpha_1+1}{2} \cdot \frac{\alpha_2+1}{2} \cdots \frac{\alpha_\nu+1}{2} \cdot \frac{\beta_{\nu+1}+1}{2} \cdot \frac{\beta_{\nu+2}+1}{2} \ldots\ldots \frac{\beta_\mu+1}{2}$$

Quotienten M', in denen kein $\beta = 0$ oder kein $r = 1$,

$$B_1 = \frac{\alpha_1+1}{2} \cdot \frac{\alpha_2+1}{2} \ldots\ldots \frac{\alpha_\nu+1}{2} \cdot \left[\frac{\beta_{\nu+2}+1}{2} \ldots\ldots \frac{\beta_\mu+1}{2} + \frac{\beta_{\nu+1}+1}{2} \cdot \frac{\beta_{\nu+3}+1}{2} \ldots\ldots \frac{\beta_\mu+1}{2} + \ldots\right]$$

Quotienten M', in denen $\mathbf{1}r = 1$,

$$B_2 = \frac{\alpha_1+1}{2} \cdot \frac{\alpha_2+1}{2} \cdots\cdots \frac{\alpha_\nu+1}{2} \cdot \left[\frac{\beta_{\nu+1}+1}{2} \cdot \frac{\beta_{\nu+4}+1}{2} \cdots\cdots \frac{\beta_\mu+1}{2} + \cdots\cdots\right]$$

Quotienten M′, in denen **2** der r = 1,

$$B_3 = \frac{\alpha_1+1}{2} \cdot \frac{\alpha_2+1}{2} \cdots\cdots \frac{\alpha_\nu+1}{2} \left[\frac{\beta_{\nu+1}+1}{2} \cdot \frac{\beta_{\nu+5}+1}{2} \cdots \frac{\beta_\mu+1}{2} + \frac{\beta_{\nu+2}+1}{2} \cdot \frac{\beta_{\nu+5}+1}{2} \cdots\cdots \frac{\beta_\mu+1}{2} + \cdots\cdots\right]$$

M′, in denen **3** der r = 1 .....

$$\cdots\cdots B_{\mu-\nu-1} = \frac{\alpha_1+1}{2} \cdot \frac{\alpha_2+1}{2} \cdots\cdots\cdots \cdots \frac{\alpha_\nu+1}{2} \left[\frac{\beta\nu+1}{2} + \frac{\beta\nu+2}{2} + \cdots + \frac{\beta\mu}{2}\right]$$

M′, in denen $_{\mu-\nu-1}$ der r = 1 und schließlich

$$B_{\mu-\nu} = \frac{\alpha_1+1}{2} \cdot \frac{\alpha_2+1}{2} \cdots \frac{\alpha_\nu+1}{2} \cdot 1$$

M′, in denen alle r = 1, gibt. Als Gesamtzal A der Zerlegungen folgt hieraus:

$$A = Bo \cdot 2^{\mu-1} + B_1 \cdot 2^{\mu-2} + B_2 \cdot 2^{\mu-3} + \cdots\cdots + B_{\mu-\nu} \cdot 2^{\mu-\nu-1} = \tfrac{1}{2}(\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\cdots(\alpha_\nu+1)\cdot(\beta_{\nu+1}+1)(\beta_{\nu+2}+1)(\beta_{\nu+3}+1)\cdots\cdots(\beta_\mu+1).$$

Diese Formel dehnt sich offenbar auch auf den Fall aus, in dem alle Exponenten ungerade werden. Dagegen muß sie sich ändern, wenn jene sämtlich gerade auftreten, M mithin ein Quadrat und das zerlegende Geschlecht das Hauptgeschlecht von D_1 wird, da sonst A eine gemischte Zahl würde. In der Tat wird dadurch ein Unterschied bedingt, daß der Quotient M′ = 1 auch einmal oder genau soviel Mal zerlegt wird wie jedes M′ mit einer noch von 1 verschiedenen Potenz.

A wird jetzt: $A = B_0 \cdot 2^{\mu-1} + B_1 \cdot 2^{\mu-2} + B_2 \cdot 2^{\mu-3} + \cdots\cdots + B_{\mu-1} \cdot 2^0 + B_\mu \cdot 2^0 \; (B_\mu = 1) = \tfrac{1}{2}(\beta_1+1)(\beta_2+1)\cdots\cdots(\beta_\mu+1) + \tfrac{1}{2} = \tfrac{1}{2}[(\beta_1+1)(\beta_2+1)\cdots\cdots(\beta_\mu+1)+1]$

Diese von Gauß (D. A. Art. 182) mit Bezug auf die besondere Form (1, 0, 1) ohne Beweis mitgeteilten Formeln verraten eine bemerkenswerte Verwandtschaft mit einer elementaren

aus der Lehre von der Teilbarkeit der Zahlen. A ist nämlich nichts anderes als die Hälfte der ungeänderten oder der um 1 vermehrten Teilerzahl von M, je nachdem M kein oder ein Quadrat ist. Prüft man die Formeln an zwei Beispielen, so mögen sämtliche Zerlegungen A von α) $M = 3969$ durch (1, 0, 5) und β) $M = 405\,589$ durch (17, 6, 17) gesucht werden. α) $3969 = 63^2 = 3^4 \cdot 7^2$ ist Rest von 5 und hat den Rest — 5, wird mithin durch (1, 0, 5) zur Darstellung gebracht. Es zeigt die Formel $A = \frac{1}{2}[5 \cdot 3 + 1]$ an. In der Tat ergeben sich die 8 Zerlegungen:

$$1 \cdot 63^2 + 5 \cdot 0^2$$
$$1 \cdot 62^2 + 5 \cdot 5^2$$
$$1 \cdot 58^2 + 5 \cdot 11^2$$
$$1 \cdot 57^2 + 5 \cdot 12^2$$
$$1 \cdot 42^2 + 5 \cdot 21^2$$
$$1 \cdot 33^2 + 5 \cdot 24^2$$
$$1 \cdot 18^2 + 5 \cdot 27^2$$
$$1 \cdot 7^2 + 5 \cdot 28^2$$

von denen, wie es die Theorie verlangt, nur 2, nämlich die 2. und 3. eigentlich, die übrigen uneigentlich sind.

β) $405\,589 = 61^2 \cdot 109$ — (17, 6, 17) vertritt das Geschlecht der Determinante $D_1 = -253$, dem der Totalcharakter 1, 4; N 11; N 23 zukommt. Da 405 589 und sein linearer Teiler 109 diesen Totalcharakter erfüllen, so wird 495 589 durch (17, 6, 17) eigentlich und uneigentlich dargestellt. Vereinigen sich jeweils die 4 Darstellungen oder die beiden Zerlegungen von S. 11, welche auf ein Paar entgegengesetzter Wurzeln der Kongruenz (A) entfallen, zu einer somit erweiterten Zerlegung, so beläuft sich die Anzahl A derselben auf

$$A = \tfrac{1}{2}[(2 + 1)(1 + 1)] = 3.$$

Zwecks ihrer Feststellung bestimmt man zunächst die Zerlegungen von $17M = 6\,895\,013$ durch die Hauptform (1, 0, 253) und bestätigt ihre formelmäßige Anzahl zu 6:

$$\begin{aligned} 6\,895\,013 &= 416^2 + 253 \cdot 163^2 \\ &= 761^2 + 253 \cdot 158^2 \\ &= 1769^2 + 253 \cdot 122^2 \\ &= 2279^2 + 253 \cdot 82^2 \\ &= 2440^2 + 253 \cdot 61^2 \\ &= 2620^2 + 253 \cdot 11^2 \end{aligned}$$

Daraus leiten sich die 3 Zerlegungen von M her:

$$\begin{aligned} 405589 &= 17 \cdot 11^2 - 2 \cdot 6 \cdot 11 \cdot 158 + 17 \cdot 158^2 \\ &= 17 \cdot 61^2 + 2 \cdot 6 \cdot 61 \cdot 122 + 17 \cdot 122^2 \\ &= 17 \cdot 163^2 - 2 \cdot 6 \cdot 163 \cdot 82 + 17 \cdot 82^2. \end{aligned}$$

Eulers Formentheorie.

a) Sätze über die allgemeine Form (a, 0, c).

Hält man der neuzeitlichen Formentheorie diejenige Eulers gegenüber, so begnügt sich diese zunächst damit, an jeder besonderen Form im wesentlichen eine Reihe allgemeiner Sätze zu wiederholen. Sie sollen an der allgemeinen Form (a, 0, c) in freier, teils hinzu-, teils wegnehmender Gestaltung vorgeführt werden.

1. Das Produkt zweier Zahlen von der Form (a, 0, c) hat auf doppelte Weise die Form (1, 0, ac); dasjenige zweier Zahlen von den Formen (a, 0, c) und (1, 0, ac) auf gleiche Weise die Form (a, 0, c); schließlich dasjenige zweier Zahlen von der Form (1, 0, ac) zwiefach die gleiche Form.

Setzt man zunächst $M_1 = ax_1^2 + cy_1^2$, $M_2 = ax_2^2 + cy_2^2$, so kommt $M_1 \cdot M_2 = (ax_1^2 + cy_1^2)(ax_2^2 + cy_2^2) =$

$$= (ax_1x_2 \pm cy_1y_2)^2 + ac(x_1y_2 \mp x_2y_1)^2 = X^2 + acY^2,$$

wenn $X = ax_1x_2 \pm cy_1y_2$ und $Y = x_1y_2 \mp x_2y_1$ eingeführt wird.

Ist $M_1 = ax_1^2 + cy_1^2$, $M_2 = x_2^2 + acy_2^2$, so wird:

$$M_1 \cdot M_2 = (ax_1^2 + cy_1^2)(x_2^2 + acy_2^2) =$$
$$= a(x_1x_2 \pm cy_1y_2)^2 + c(ax_1y_2 \mp x_2y_1)^2 =$$
$$= aX^2 + cY^2, \text{ falls } X = x_1x_2 \pm cy_1y_2,\ Y = ax_1x_2 \mp x_2y_1$$

substituiert wird.

Ist schließlich $M_1 = x_1^2 + acy_1^2$, $M_2 = x_2^2 + acy_2^2$, so ist $M_1M_2 = (x_1x_2 \pm acy_1y_2)^2 + ac(x_1y_2 \mp x_2y_1)^2$, oder

$$X \text{ für } x_1x_2 \pm acy_1y_2,\quad Y \text{ für } x_1y_2 \mp x_2y_1$$

gesetzt, $= X^2 + acY^2$.

Man kann hinzufügen: Sind M_1 und M_2, x_1 und y_1, x_2 und y_2 zueinander prim, dann sind es auch X und Y.

Denn nimmt man im ersten Falle für

$$\left| \begin{matrix} x_2, & y_2 \\ y_1, & x_1 \end{matrix} \right| \quad X = ax_1x_2 \pm cy_1y_2,\ Y = x_1y_2 \mp x_2y_1 \quad \left| \begin{matrix} cy_2, & ax_2 \\ ax_1, & cy_1 \end{matrix} \right|$$

das Gegenteil an, so wäre ein gemeinsamer Teiler von X und Y auch in

$$\begin{aligned} Xx_2 + cYy_2 &= x_1(ax_2^2 + cy_2^2) \\ Xy_2 - aYx_2 &= \pm y_1(ax_2^2 + cy_2^2) \\ Xx_1 \mp cYy_1 &= x_2(ax_1^2 + cy_1^2) \\ Xy_1 \pm aYx_1 &= \pm y_2(ax_1^2 + cy_1^2), \end{aligned}$$

mithin in M_1 und M_2 oder in M_1, x_2 und y_2 oder schließlich in M_2, x_1 und y_1 enthalten, welche Schlüsse der Voraussetzung zuwiderlaufen. Mithin besteht die Behauptung zu Recht. Analog bestätigt sie sich auch für die übrigen beiden Fälle.

2. Eine mehrmals in die Form (a, 0, c) eingehende Zahl M ist notwendig zusammengesetzt.

Dem auf S. 10 geführten Beweise möge noch der Eulersche beigefügt werden. Es sei

(1) $M = ax_1^2 + cy_1^2 \mid x_2^2, y_2^2$ (2) $M = ax_2^2 + cy_2^2 \mid x_1^2, y_1^2$

Multipliziert man (1) mit x_2^2, bzw. y_2^2; (2) mit x_1^2, bzw. y_1^2, und subtrahiert dann beidemale (1) von (2), so erhält man die beiden Gleichungen:

(3): $M(x_1 - x_2)(x_1 + x_2) = c(x_1y_2 - x_2y_1)(x_1y_2 + x_2y_1)$

(4): $M(y_1 - y_2)(y_2 + y_2) = a(x_2y_1 - x_1y_2)(x_2y_1 + x_1y_2)$

Da $2M = ax_1^2 + cy_1^2 + ax_2^2 + cy_2^2$, $2(M - x_1y_2 - x_2y_1) = (x_1 - y_2)^2 + (x_2 - y_1)^2 + (a-1)(x_1^2 + x_2^2) + (c-1)(y_1^2 + y_2^2)$ ist, so folgt, daß, sobald nur die Zerlegungen voneinander verschieden sind, $M > x_1y_2 + x_2y_1$ ist. Unter Ausschluß der Werte $M = a, c$ kann also M in keinem der 3 Faktoren der rechten Seite von (3) und (4) vollständig, sondern nur teilweise enthalten sein, was ein primes M widerlegt.

3. Faktorenbestimmung einer solchen Zahl M.

Unter der gleichen Voraussetzung wie in (2) folgt:

$$a(x_1^2 - x_2^2) = -c(y_1^2 - y_2^2); \quad \frac{x_1 \pm x_2}{y_1 \pm y_2} = -\frac{c}{a} \cdot \frac{y_1 \mp y_2}{x_1 \mp x_2}.$$

Ersetzt man den letzten Bruch durch den möglichst gekürzten $\frac{p}{q}$ so wird man ansetzen

$$(1)\ \begin{matrix} x_1 \pm x_2 = mp; & y_1 \mp y_2 = -nap \\ y_1 \pm y_2 = mq; & x_1 \mp x_2 = -ncq \end{matrix}; \text{ daraus } \begin{matrix} (2a)\ 2x_1 = mp + ncq \\ (2b)\ 2y_1 = mq - nap \end{matrix}$$

$$(F): M = a\left(\frac{mp + ncq}{2}\right)^2 + c\left(\frac{mq - nap}{2}\right)^2 = \tfrac{1}{4}(m^2 + acn^2)(ap^2 + cq^2)$$

Ist n ganz, dann ist der ungerade Bestandteil von $ap^2 + cq^2$ ein Teiler von M. Ist aber n gebrochen, $n = \frac{n'}{n''}$, so ist n'' in ap und cq als ihr größter gemeinschaftlicher Teiler enthalten. Bedeutet ferner $\frac{a'c'}{v}$ den nach Möglichkeit gehobenen Bruch $\frac{ac}{n''}$, so geht v in p und q auf. Indem also die 2. Klammer durch $n'' \cdot v$ teilbar wird, dividiert man sie durch $n'' \cdot v$, während man die 1. Klammer mit $n'' \cdot v$ multipliziert. Dadurch zerlegt sich M, abgesehen von dem Anfangsbruch, in ganze Faktoren.

$$(F'): \quad M = \tfrac{1}{4}\,(m^2 n'' v + a'c'n'^2)\left(\frac{ap}{n''} \cdot \frac{p}{v} + \frac{cq}{n''} \cdot \frac{q}{v}\right)$$

Die 2. Klammer kann für ein ungerades M und relativ prime a und c niemals durch 4 teilbar sein. Denn nimmt man an:

1. alle 4 Größen a, c, p und q sind ungerade, dann müssen m und n′ beide entweder gerade oder ungerade, mithin beide Klammern gerade werden;

2. eine der 4 Größen ist gerade, dann erhält die 2. Klammer sicher einen ungeraden Wert;

3. 2 Größen, etwa a und q sind gerade; dadurch wird es auch n''. Enthält nun q die größere oder gleiche Potenz der 2 wie a, so bedingt (2b) ein gerades n′; enthält q die kleinere Potenz, so bedingt (2b) ein gerades a′.

Folglich erhellt, daß stets die 1. Klammer gerade ausfällt, und somit die Richtigkeit der Behauptung. Aus je 2 Zerlegungen $(x_1\ y_1)$ und $(x_2\ y_2)$ von M in (a, 0, c) gehen also infolge vierfacher Kombination der Vorzeichen 8 Faktoren von M hervor, die aber gewöhnlich teilweise zusammenfallen. Euler stützt sich hierin auf Induktion; einen allgemeinen Zusammenhang zwischen der Anzahl der Zerlegungen und derjenigen der Primteiler von M kennt er nicht. Um die 8 Faktoren von M zu ermitteln, gibt man dem Bruche $\frac{x_1 \pm x_2}{y_1 \pm y_2}$ in $\frac{p}{q}$, hernach dem andern $\frac{ap^2}{cq^2}$ in $\frac{p'}{q'}$ seine einfachste Gestalt. Dann stellt $m = p' + q'$ oder, falls $p' + q'$ gerade ist, $\frac{m}{2}$ auf jeden Fall einen Teiler von M dar (vgl. auch Seelhoff, Amer. Journal of Math. Vol. VII S. 266). Mit m, bzw. $\frac{m}{2}$ paart

man den weiteren Faktor $m' = \frac{M}{m}$, bzw. $\frac{2M}{m}$. Für die einfachsten Formen (1, 0, 1) (a = c = 1) und (1, 0, 2) (a = 1, c = 2) gibt Formel (F) die Faktorenzerlegung (F_{-1}): $M = \frac{1}{4}(m^2 + n^2)(p^2 + q^2) = \frac{1}{4} m_1 m_2$ und (F_{-2}): $M = \frac{1}{4}(m^2 + 2n^2)(p^2 + 2q^2) = \frac{1}{4} m_1 m_2$. Da in ($F_{-1}$) n stets ganz sein muß, gilt dies auch von den beiden Klammerwerten. Je nachdem die Quadrate beide ungerade; das eine ungerade, das andere gerade oder schließlich beide gerade sind, hat ihre Summe bzw. die Form 4n + 2, 4n + 1 oder 4n. Da also die beiden Faktoren m_1 und m_2 entweder beide ungerade gerade oder m_1 gerade gerade, m_2 ungerade sein müssen, so werden dadurch im ersten Falle je 2 ungerade Quadrate von m_1 und m_2; im letzten 2 gerade Quadrate von m_1 bedingt, d. h. in beiden Fällen verschwindet der Nenner 4, ohne daß die Gestalt der andern Faktoren sich ändert:

$$(F'_{-1}):\ M = \left(\left(\frac{m+n}{2}\right)^2 + \left(\frac{m-n}{2}\right)^2\right)\left(\left(\frac{p+q}{2}\right)^2 + \left(\frac{p-q}{2}\right)^2\right) \text{ und}$$

$$M = (m'^2 + n'^2)(p^2 + q^2)$$

Der in (F_{-2}) mögliche Nenner $n'' = 2$ schließt sich dadurch aus, daß er $x_1 \pm x_2$ gleichzeitig einen geraden und einen ungeraden Wert erteilen würde. Da die Summe eines einfachen und eines doppelten Quadrates von der Form α) 8n + 0, 4 β) 8n + 3 γ) 8n + 1 und δ) 8n + 2 (6) ist, je nachdem α) beide Quadrate gerade β) beide ungerade γ) das einfache ungerade, das doppelte gerade und δ) umgekehrt sind, so müssen wie oben entweder beide Faktoren m_1 und m_2 ungerade gerade oder m_1 gerade gerade, m_2 ungerade werden. In jenem Falle läßt sich substituieren: $m = 2m'$, $p = 2p'$; in diesem $m = 2m'$, $n = 2n'$, womit M beidemale auf ein Produkt 2er Faktoren der Form $a^2 + 2c^2$ zurückgeführt wird. Während somit die aus den Zerlegungen von M in die allgemeine Form (a, 0, c) entspringenden Faktoren i. A. mit M nicht in jener Form übereinstimmen, trifft dies für die besonderen Formen (1, 0, 1) und (1, 0, 2) zu. Durch ein Reduktionsverfahren (vgl. C 1, 12 S. 161; C 1, 13, S. 184) beweist Euler, daß jeder Teiler und mithin auch alle Primteiler einer Zahl M von der Form (1, 0, 1) oder (1, 0, 2) in der gleichen Form enthalten sein müssen, sobald sie es nicht schon in den Unbestimmten dieser Formen sind. Es gelingt ihm aber nur teilweise, den Zusammenhang zwischen jenen quadratischen

und den ihnen entsprechenden linearen nachzuweisen, nämlich daß jede Primzahl von der Form $4n + 1$ einmal in (1, 0, 1), eine solche von den Formen $8n + 1$, 3 einmal in (1, 0, 2) eingeht. In C 1, 15 holt er die Begründung des ersten Satzes, die er in C 1, 12 selber als einen bloßen Versuch (tentamen demonstrationis) wertet, nach; diejenige des letzten Satzes ist ihm nie vollständig geglückt.

4. Wird eine Zahl M der Form (a, 0, c) mit relativ primen a u. c durch eine andere prime M_1 gleicher Form oder dieser (1, 0, ac) geteilt, so besitzt der Quotient M_2 die Form (1, 0, ac), bzw. (a, 0, c).

α) Es sei $M = ax^2 + cy^2$, $M_1 = ax_1^2 + cy_1^2$

$$M \cdot M_1 = (axx_1 \pm cyy_1)^2 + ac(xy_1 \mp x_1y)$$

$$(G)\quad \frac{ax^2 + cy^2}{ax_1^2 + cy_1^2} = \left(\frac{axx_1 \pm cyy_1}{ax_1^2 + cy_1^2}\right)^2 + ac\left(\frac{xy_1 \mp x_1y}{ax_1^2 + cy_1^2}\right)^2$$

$$ax^2 + cy^2 = (ax_1^2 + cy_1^2)M_2 = ax_1^2 \cdot M_2 + cy_1^2 \cdot M_2.$$

Die Summanden der beiden Seiten können sich nur um das kleinste gemeinschaftliche Vielfache von a u. c, d. h. um das Produkt ac, oder ein Vielfaches desselben unterscheiden. Mithin ist die Substitution begründet:

$$\begin{array}{rcl|l} x^2 + k \cdot c & = & x_1^2 \cdot M_2 & y_1^2 \\ y^2 - k \cdot a & = & y_1^2 \cdot M_2 & x_1^2 \end{array}$$

Multipliziert man die obere Gleichung mit y_1^2, die untere mit x_1^2 und subtrahiert jene von dieser, so ist: $x_1^2y^2 - x^2y_1^2 = kax_1^2 + kcy_1^2$ oder $(x_1y + xy_1)(x_1y - xy_1) = k(ax_1^2 + cy_1^2)$; da nun nach Voraussetzung $M_1 = ax_1^2 + cy_1^2$ prim ist, so muß es entweder in $x_1y + xy_1$ oder in $x_1y - xy_1$ aufgehen; damit aber werden die beiden rechtsseitigen Brüche in (G) ganze Zahlen, und M_2 erscheint in der Form (1, 0, ac).

$$(\alpha')\ M = ax^2 + cy^2,\ M_1 = x_1^2 + acy_1^2$$

$$MM_1 = a(xx_1 \pm cyy_1)^2 + c(axy_1 \mp x_1y)^2$$

$$(G')\quad \frac{ax^2 + cy^2}{x_1^2 + acy_1^2} = a\left(\frac{xx_1 \pm cyy_1}{x_1^2 + acy_1^2}\right)^2 + c\left(\frac{axy_1 \mp x_1y}{x_1^2 + acy_1^2}\right)^2$$

Dann: $ax^2 + cy^2 = x_1^2 \cdot M_2 + acy_1^2 \cdot M_2$. Die Vielfachen von a können nur um ein solches von einander abweichen, mithin führt man ein:

$$\begin{array}{rcl|l} x^2 + k & = & cy_1^2 \cdot M_2 & x_1^2 \\ cy^2 - k \cdot a & = & x_1^2 \cdot M_2 & cy_1^2 \end{array}$$

Multipliziert man die obere Gleichung mit x_1^2, die untere mit cy_1^2 und zieht diese von jener ab, so folgt:

$$x^2x_1^2 - c^2y^2y_1^2 = -k(x_1^2 + acy_1^2)$$

Da $x_1^2 + acy_1^2 = M_1$ als prim angenommen ist, muß M_1 entweder in $xx_1 + cyy_1$ oder in $xx_1 - cyy_1$ aufgehen, d. h. die beiden rechtsstehenden Brüche in (G′) nehmen ganzzahlige Werte an, M_2 somit die Form (a, 0, c). Ist M_1 zusammengesetzt, so besteht der Satz nur, falls beidemale entweder die Summe oder die Differenz prim zu M_1 ist.

Die beiden Eulerschen Hauptmethoden.

Die Tauglichkeit zur Untersuchung der Primzahlen schneidet in den Formenkomplex (a, 0, c) eine große Kluft ein, die zuerst von Euler festgestellt, jedoch im Kerne nur induktiv begründet wurde. Während nämlich die Allgemeinheit der Formen (a, 0, c) an keine mehrmalige Wiedergabe einer zusammengesetzten Zahl, der sie sich überhaupt zugänglich erweist, gebunden ist, zeichnen sich einige wenige, worunter auch die einfachsten (1, 0, 1) und (1, 0, 2) zählen, durch die entgegengesetzte Eigenschaft aus. Ehe die Entdeckung Eulers, der Gipfelpunkt seiner Formentheorie, weiter verfolgt werden soll, mögen seine ersten beiden Methoden der Primzahlbestimmung, die sich auf die Formen (1, 0, 1) und (1, 0 2) stützen, mit ihren Erweiterungen entwickelt werden.

1. Die besondere theoretische Grundlage der beiden Methoden.

Der Grundpfeiler, auf den sie aufgebaut sind, ist der Satz, daß jede Primzahl der linearen Form $4n + 1$ einmal in die quadratische (1, 0, 1), eine solche der linearen Formen $8n + 1$ oder $8n + 3$ einmal in die quadratische (1, 0, 2) eingeht. Ist also die vorgelegte Zahl M von einer jener linearen Formen und 1) prim, so wird sie notwendig durch (1, 0, 1) bzw. (1, 0, 2) auf eine einzige Art zerlegt. 2) Ist aber M zusammengesetzt, so spaltet sich M allgemeinen Falls in 2 Faktoren m_1 u. m_2, von denen der eine m_1 nur Primteiler in der linearen Form von M, der andere m_2 solche der einzelnenfalls noch möglichen linearen Formen, nämlich $4n - 1$, bzw. $8n - 1$ u. $8n - 3$, in gerader Menge umfaßt. Nach obigem Hauptsatze können diese für sich durch (1, 0, 1), bzw. (1, 0, 2) nicht zerlegt werden, sondern ihr Produkt m_2 muß, wie es am Ende des vorigen

Satzes 3) angedeutet wurde, in den quadratischen Unbestimmten aller Zerlegungen von M aufgehen, was m_2 Quadratform vorschreibt. Sie können demnach die Anzahl der letzteren nicht beeinflussen, vielmehr fällt diese mit derjenigen der Zerlegungen von m_1 zusammen. α) Besteht m_1 aus lauter gleichen Primteilern, ist es also eine Primzahlpotenz, $m_1 = p^\mu$, so zeigt Euler induktiv an der Entwicklung der ersten Potenzen von p, daß p^μ genau soviel Mal wie p, d. h. nur einmal eigentlich zerlegt wird. Denn setzt man das eine Mal $p = x^2 + y^2$, so folgt:

a) $p^2 = 0^2 + (x^2 + y^2)^2$
b) $p^2 = (2xy)^2 + (x^2 - y^2)^2$
c) $p^3 = (x^3 + xy^2)^2 + (x^2y + y^3)^2$
d) $p^3 = (x^3 - 3xy^2)^2 + (y^3 - 3x^2y)^2$
e) $p^4 = 0^2 + (x^4 + 2x^2y^2 + y^4)^2$
f) $p^4 = (2x^3y + 2xy^3)^2 + (x^4 - y^4)^2$
g) $p^4 = (4x^3y - 4xy^3)^2 + (x^4 - 6x^2y^2 + y^4)^2$

. . . . . .

In a), c) und f) haben die Unbestimmten den Faktor $(x^2 + y^2)$, in e) den Faktor $(x^4 + 2x^2y^2 + y^4)$ gemein, sodaß für jede Potenz in der Tat nur eine eigentliche Zerlegung zurückbleibt. Nimmt man das zweite Mal an: $p = x^2 + 2y^2$, so entwickelt man:

a) $p^2 = (x^2 + 2y^2)^2 + 2 \cdot 0^2$
b) $p^2 = (2y^2 - x^2)^2 + 2(2xy)^2$
c) $p^3 = (x^3 + 2xy^2)^2 + 2(x^2y + 2y^3)^2$
d) $p^3 = (6xy^2 - x^3)^2 + 2(2y^3 - 3x^2y)^2$
e) $p^4 = (x^4 + 2x^2y^2 + y^4)^2 + 2 \cdot 0^2$
f) $p^4 = (x^4 - 4y^4)^2 + 2(2x^3y + 4xy^3)^2$
g) $p^4 = (x^4 - 12x^2y^2 + y^4)^2 + 2(4x^3y - 8xy^3)^2$

. . . . . .

Indem in a), c) und f) die Unbestimmten den Teiler $(x^2 + 2y^2)$, in e) den Teiler $(x^4 + 2x^2y^2 + y^4)$ enthalten, wiederholt sich die vorige Beobachtung. p^μ kann sich noch verdoppeln, ohne daß die Zahl seiner Zerlegungen sich ändert. Denn jede weitere von $2 \cdot p^\mu$ würde eine solche von p^μ nach sich ziehen. Aus $2 \cdot p^\mu = x^2 + y^2$ oder $x^2 + 2y^2$ folgt nämlich unmittelbar:

$$p^\mu = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2, \text{ bzw.}$$

$$= y^2 + 2 \cdot \left(\frac{x}{2}\right)^2.$$

β) Setzt sich m_1 aus μ verschiedenen Primfaktoren in verschiedenen Potenzen: $m_1 = p_1^{\alpha_1} p_2^{\alpha_2} \ldots . p_\mu^{\alpha_\mu}$ zusammen, so entfällt auf jede Potenz eine eigentliche Zerlegung durch (1, 0, 1), bezw. (1, 0, 2). Leicht entnimmt man hieraus, was Euler unterläßt, die Menge A′ aller eigentlichen Zerlegungen von m_1. Gemäß Satz 1, S. 19 entstehen aus denjenigen von $p_1^{\alpha_1}$ und $p_2^{\alpha_2} 2^1$ eigentliche Zerlegungen ihres Produktes $p_1^{\alpha_1} \cdot p_2^{\alpha_2}$, aus diesen und der von $p_3^{\alpha_3} 2^2$ eigentliche Zerlegungen von $p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$ u. s. f. Auf diese Weise das vollständige Produkt bildend, erkennt man in A′ den Wert $2^{\mu-1}$, den auch die neuere Zahlentheorie an die Hand gibt. Die Anzahl A sämtlicher, sowohl der eigentlichen, als auch der uneigentlichen Zerlegungen von m_1 und damit aller derer von M beläuft sich nach S. 18 auf:

$$A = \tfrac{1}{2} [(\alpha_1 + 1)\ (\alpha_2 + 1)\ \alpha_3 + 1) \ldots (\alpha_\mu + 1) + \epsilon],$$

wo $\epsilon = 0$ oder $= 1$ ist, je nachdem m_1 und somit M kein oder ein Quadrat ist. Unter Beschränkung auf eigentliche Zerlegungen gelangt man also zu folgendem Ergebnis: Wird M überhaupt nicht zerlegt, dann ist es sicherlich nicht prim, sondern enthält einen nichtquadratischen Faktor m_2. Findet eine einmalige Zerlegung statt, so ist M prim oder primäquivalent, d. h. eine einfache oder doppelte Primzahlpotenz; ergibt sich endlich eine mehrmalige Zerlegung, so setzt sich M aus verschiedenen Primteilern zusammen. Da umgekehrt jedes prime M einfach, jedes zusammengesetzte dagegen mehrfach durch (1, 0, 1), bezw. (1, 0, 2) zerlegt werden muß, so sind diese Formen zur Untersuchung des primen oder zusammengesetzten Charakters aller Zahlen M, d. h. aller derer geeignet, die in die zugehörigen linearen Formen $4n + 1$, bezw. $8n + 1$ oder $8n + 3$ eingehen. Jede der beiden Formen kann also auf die Hälfte aller ungeraden Zahlen bezogen werden. Wie schon vorausgeschickt wurde, befolgt Euler in allen seinen Arbeiten über Primzahlbestimmung eine Subtraktionsmethode. Obwohl diese stets dasselbe einfache Prinzip einhält, ist doch ihre Ausführung an den einzelnen Formen (a, 0, c) verschieden, weshalb eine Einteilung ihrer Darstellung nach diesen Formen geboten ist.

2. Primzahlbestimmung mittels der Form (1, 0, 1).

Ihr unterwirft sich jede Zahl $M \equiv 1 \pmod 4$. Man bildet alle möglichen Differenzen $M - y^2$ und behält unter ihnen die quadratischen bei. Soviele solcher vorhanden sind, soviele Zerlegungen von M in 2 Quadrate haben statt. Durch folgende Erwägung vermindert sich aber die Zahl der Subtraktionen. Da jede Quadratzahl auf eine der Ziffern 0, 1, 4, 5, 6, 9 ausgeht, so wird die Subtraktion aller derjenigen Quadrate y^2 als zwecklos unterbleiben, die der Differenz $M - y^2$ eine der andern Endziffern erteilt. Mit jeder der Primzahlendziffern 1, 3, 7, 9 vertragen sich nur bestimmte Quadrat- und damit auch nur bestimmte Quadratwurzelendziffern. Den Zusammenhang zwischen den 3 Gattungen von Endziffern veranschaulicht nachstehende Tabelle (vgl. C 1, 12 S. 167):

Primzahlendz. z_1	Quadratendz. z_2	Quadratwurzelendz. z_3
1	0, 1, 5, 6	0, 1, 4, 5, 6, 9
3	4, 9	2, 3, 7, 8
7	1, 6	1, 4, 6, 9
9	0, 4, 5, 9	0, 2, 3, 5, 7, 8

Jeder zulässigen Endziffer z_3 ordnet man eine besondere Reihe von Subtraktionen zu, d. h. man zieht in einer Folge von M alle diejenigen Quadrate ab, deren Wurzeln in der Endziffer z_3 übereinstimmen und somit im Abstande von 10 aufeinander folgen. Sie bilden, wie untenstehender Ausschnitt darlegt, eine arithmetische Reihe 2. Ordnung mit der konstanten Differenz.

$$\pm 200:$$

$$[k \cdot 10 + z_3]^2 \quad [(k \pm 1)\,10 + z_3]^2 \quad [(k \pm 2)\,10 + z_3]^2 \quad [(k \pm 3)\,10 + z_3]^2$$

$$20\,(k + z_3) \pm 100 \quad 20\,(k + z_3) \pm 300 \quad 20\,(k + z_3) \pm 500$$

$$\pm 200 \qquad \pm 200$$

Beginnt man also mit der Subtraktion des größtmöglichen derartigen Quadrates y_0^2, so fügt man zu der Differenz $M - y_0^2$ $20y_0 - 100$ hinzu, um die nächste $M - (y_0 - 10)^2$, zu dieser $20y_0 - 300$, um die übernächste usf. zu erhalten. Die Summandenkette stellt die 1. Differenzenreihe zu der quadratischen Subtrahendenkette dar; als solche hat sie die konstante Differenz

— 200 und ist folglich sofort angebbar. Ist die Differenz $x^2 = M - y^2$, die ebenso wie ihr Subtrahend stets mit gleicher Endziffer auftritt, von ihrem kleinsten Werte bis zur Hälfte von M gestiegen, so unterbricht man die Reihe. Denn nach dermaßen vollendeter Rechnung könnten nur noch Zerlegungen ausstehen, in denen beide Quadrate $> \frac{M}{2}$ wären, was widersinnig ist, da in jeder Zerlegung von M das eine Quadrat oberhalb, das andere unterhalb $\frac{M}{2}$ liegen muß. An die Differenzenreihen mit den Endziffern 0 und 5 schließt noch die Bemerkung an, daß unter ihren Gliedern nur diejenigen taugen, die vor 0 und 5 noch eine 0, bzw. eine 2 nehmen. Bezeichnet wiederum x_0^2 das größtmögliche Quadrat, das der Differenz y^2 das Endziffernpaar 00, bzw. 25 verleiht, selber aber nicht auf 0 oder 5 ausgehen kann, so ist offensichtlich, daß nur die Quadrate $(x_0 - 50)^2$, $(x_0 - 100)^2$, $(x_0 - 150)^2$ ..... gleicherweise wirken, die dazwischenliegenden aber übergangen werden können. Da die Summanden, die allgemein die Differenz $M - (x_0 - m \cdot 50)^2$ zur nächstfolgenden $M - [x_0 - (m + 1)\ 50]^2$ vergrößern, nämlich $100x_0 - 2500 - m \cdot 5000$ eine arithmetische Reihe 1. Ordnung mit der Differenz — 5000 und dem Anfangsgliede $100x_0 - 2500$ bilden, so geht die Gliederzahl solcher Subtraktionsketten erheblich zurück. Da zu $z_1 = 1$ und $= 9$ je 2 solche, außerdem aber noch 4 andere gehören, so gleicht sich die rechnerische Arbeit für alle 4 Arten von Primzahlen einigermaßen aus. Ein von Euler nicht behandeltes Beispiel möge seine Methode erproben. Gegeben sei M = 214 693. Mithin $z_1 = 3$; $z_3 = 2, 3, 7, 8$; 4 Subtraktionsreihen werden eingerichtet.

M = 214 693	M = 214 693	M = 214 693	M = 214 693
$-462^2 = 213\,444$	$-463^2 = 214\,369$	$-457^2 = 208\,849$	$-458^2 = 209\,764$
1 249	$18^2 =$ 324	5 844	4 929
+ 9 140	+ 9 160	+ 9 040	+ 9 060
10 389	9 484	$122^2 =$ 14 884	13 989
+ 8 940	+ 8 960	+ 8 840	+ 8 860
19 329	18 444	23 724	22 849
+ 8 740	+ 8 760	+ 8 640	+ 8 660
28 069	27 204	32 364	31 509
+ 8 540	+ 8 560	+ 8 440	+ 8 460

36 609	35 764	$202^2 = 40\,804$	39 969
+ 8 340	+ 8 360	+ 8 240	+ 8 260
44 949	44 124	49 044	48 229
+ 8 140	+ 8 160	+ 8 040	+ 8 060
53 089	52 284	57 084	56 289
+ 7 940	+ 7 960	+ 7 840	+ 7 860
61 029	60 244	64 924	64 149
+ 7 740	+ 7 760	+ 7 640	+ 7 660
68 769	68 004	72 564	71 809
+ 7 540	+ 7 560	+ 7 440	+ 7 460
76 309	75 564	80 004	79 269
+ 7 340	+ 7 360	+ 7 240	+ 7 260
83 649	82 924	87 244	86 529
+ 7 140	+ 7 160	+ 7 040	+ 7 060
90 789	90 084	94 284	93 589
+ 6 940	+ 6 960	+ 6 840	+ 6 860
97 729	97 044	$318^2 = 101\,124$	100 449
+ 6 740	+ 6 760		
104 469	103 804		

Die Tabelle liefert 4 Zerlegungen von 214 693 in (1, 0, 1):

$$\begin{aligned} 214\,693 &= 18^2 + 463^2 \\ &= 122^2 + 447^2 \\ &= 202^2 + 417^2 \\ &= 318^2 + 337^2 \end{aligned}$$

Aus den Brüchen $\frac{463 + 417}{202 + 18} = \frac{4}{1}$, $\frac{447-417}{202-122} = \frac{3}{8}$, $\frac{463-447}{122-18} = \frac{2}{13}$ folgen bezw. die Primfaktoren $1^2 + 4^2 = 17$, $3^2 + 8^2 = 73$, $2^2 + 13^2 = 173$.

3. Primzahlbestimmung durch (1, 0, 2).

Sie gleicht der vorigen darin, daß die Subtraktionen in mehreren getrennten Reihen verlaufen, in denen Subtrahenden und Differenzen für sich in der Endziffer übereinstimmen und arithmetische Reihen 2. Ordnung bilden; unterscheidet sich aber von ihr darin, daß nicht die einfachen, sondern die doppelten Quadrate und nicht in absteigender, sondern in aufsteigender Reihe abgezogen werden. M hat entweder die Form $8n + 1$ oder $8n + 3$. In jenem Falle werden nur die geraden, in

diesem nur die ungeraden Doppelquadrate abgezogen. In allen beiden ordnen sich diese in 5 Reihen ein, von denen jede gleiche Wurzelendziffer wahrt. Jede stellt ferner, wie nachfolgende Entwicklung darlegt, eine arithmetische Reihe 2. Ordnung dar, deren konstante Differenz doppelt so groß als die in der vorigen Methode ist.

$$\begin{array}{ccccc} 2[k\cdot 10+z_3]^2 & 2[(k\pm 1)10+z_3]^2 & 2[(k\pm 2)10+z_3]^2 & 2[(k\pm 3)10+z_3]^2 \\ 40(k+z_3)\pm 200 & 40(k+z_3)\pm 600 & 40(k+z_3)\pm 1000 \\ \pm 400 & \pm 400 \end{array}$$

Bedeutet ferner $2y_0^2$ das kleinste Doppelquadrat der Reihe, so gibt eine zweite Zusammenstellung ihren Anfang wieder:

$$\begin{array}{ccccc} 2y_0^2 & 2(y_0+10)^2 & 2(y_0+20)^2 & 2(y_0+30)^2 & 2(y_0+40)^2 \\ 40y_0+200 & 40y_0+600 & 40y_0+1000 & 40y_0+1400 \\ 400 & 400 & 400 \end{array}$$

Zunächst zieht man von M $2y_0^2$, hierauf von der Differenz $M-2y_0^2$ $40y_0+200$, von der neuen Differenz $40y_0+600$, von der weiteren $40y_0+1000$ u.s.f. ab und untersucht allemal die Differenz $M-2y^2$ auf ihren quadratischen Charakter. Zwei Bemerkungen, die Euler nicht besonders hervorhebt, tragen zur wesentlichen Vereinfachung des Rechnungsverfahrens bei. 1) 2 der 5 Subtrahendenreihen endigen auf 2, 2 andere auf 8, die letzte auf 0. Da M mit einer der 4 Ziffern 1, 3, 7, 9 schließen muß, so fallen im 1. und 4. Falle die beiden Subtrahendenreihen auf 8, bezw. 2; im 2. und 3. Falle diejenige auf 0 weg. 2) Eine Differenzenreihe mit der Endziffer 0 oder 5 erleidet dieselbe Einschränkung wie in der vorigen Methode. Stellt aufs neue $2y_0^2$ das kleinste Doppelquadrat vor, das der Differenz $M-2y^2$ das Endziffernpaar 00 oder 25 gibt, so behält man von der Reihe nur die Quadrate bei:

$$2y_0^2,\quad 2(y_0+50)^2,\quad 2(y_0+100)_2\ldots\quad 2(y_0+n\cdot 50)^2\ldots,$$

die sich zu einer arithmetischen Reihe 2. Ordnung mit der konstanten Differenz 10 000 zusammenschließen, wie die Differenzbildung zeigt:

$$\begin{array}{ccccc} 2y_0^2 & 2(y_0+50)^2 & 2(y_0+100)^2 & 2(y_0+150)^2\ldots \\ 200y_0+5000 & 200y_0+15\,000 & 200y_0+25\,000 \\ 10\,000 & 10\,000 \end{array}$$

Da sich den Primzahlen auf 3 und 7 je 2 solcher Differenzenreihen zuordnen, sie aber sonst nur eine Subtrahendenreihe

ablehnen, so wiederholt sich, daß die Methode für alle untersuchten Zahlen nahezu die gleiche Arbeit beansprucht. 3 von Euler nicht gewählte Beispiele werden die Wirksamkeit seiner 2. Methode beurteilen lassen.

α) $M = 8n + 3 = 81\,371.$

Abgezogen werden die beiden Subtrahendenreihen auf 2 und die auf 0.

M = 81 371	81 371	81 371
— 2	50	162
81 369	81 321	81 209
— 240	400	560
81 129	80 921	80 649
— 640	800	960
80 489	80 121	79 689
— 1 040	1 200	1 360
79 449	78 921	78 329
— 1 440	1 600	1 760
78 009	77 321	76 569
— 1 840	2 000	2 160
76 169	75 321	74 409
— 2 240	2 400	2 560
73 929	72 921	71 849
— 2 640	2 800	2 960
267^2 = 71 289	70 121	68 889
— 3 040	3 200	3 360
68 249	66 921	65 529
— 3 440	3 600	3 760
64 809	63 321	61 769
— 3 840	4 000	4 160
60 969	59 321	57 609
— 4 240	4 400	4 560
56 729	54 921	53 049
— 4 640	4 800	4 960
52 089	50 121	48 089
— 5 040	5 200	5 360
47 049	44 921	42 729
— 5 440	5 600	5 760
41 609	39 321	36 969
— 5 840	6 000	6 160
35 769	33 321	30 809
— 6 240	6 400	6 560
29 529	26 921	24 249
— 6 640	6 800	6 960

22 889	20 121	17 289
— 7 040	7 200	7 360
15 849	12 921	9 929
— 7 440	7 600	7 760
8 409	5 321	2 169
— 7 840		
569		

Die Rechnung liefert nur eine Zerlegung von 81 371 in (1, 0, 2):

$$81\,371 = 267^2 + 2 \cdot 71^2.$$

mithin ist 81 371 eine Primzahl.

β) $M = 8n' + 1 = 164\,537.$

Zum Abzug kommen die beiden Subtrahendenreihen auf 2 und die auf 8. Zu jenen gehören Differenzenreihen auf 5, deshalb werden sie verkürzt abgezogen.

M = 164 537	164 537	164 537
— 8	2 312	128
164 529	162 225	164 409
— 280	11 800	520
164 249	150 425	163 889
— 680	21 800	920
163 569	128 625	162 969
— 1 080	31 800	1 320
162 489	96 825	161 649
— 1 480	41 800	1 720
161 009	55 025	159 929
— 1 880	51 800	2 120
159 129	3 225	157 809
— 2 280		2 520
156 849	164 537	155 289
— 2 680	512	2 920
154 169	$405^2 = 164\,025$	152 369
— 3 080	8 200	3 320
151 089	155 825	149 049
— 3 480	18 200	3 720
147 609	137 625	145 329
— 3 880	28 200	4 120
143 729	109 425	141 209
— 4 280	38 200	4 520
139 449	71 225	136 689
— 4 680	48 200	4 920

134 769	23 025	$363^2 = 131\,769$
— 5 080		5 320
129 689		126 449
— 5 480		5 720
124 209		120 729
— 5 880		6 120
118 329		114 609
— 6 280		6 520
112 049		108 089
— 6 680		6 920
105 369		101 169
— 7 080		7 320
98 289		93 849
— 7 480		7 720
90 809		86 129
— 7 880		8 120
82 929		78 009
— 8 280		8 520
74 649		69 489
— 8 680		8 920
65 969		60 569
— 9 080		9 320
56 889		51 249
— 9 480		9 720
47 409		41 529
— 9 880		10 120
37 529		31 409
— 10 280		10 520
27 249		20 889
— 10 680		10 920
16 569		9 969
— 11 080		
5 489		

Man hat also

$$164\,537 = 363^2 + 2 \cdot 128^2$$
$$= 405^2 + 2 \cdot 16^2.$$

Aus dem Bruche $\frac{405 \pm 363}{128 \pm 16}$ fließen die Teiler $3^2 + 2 \cdot 8^2 = 137$; $7^2 + 2 \cdot 24^2 = 1201$, in der Tat $164\,537 = 137 \cdot 1201$.

γ. $M = 8n'' + 1 = 78\,217$.

Zur Subtraktion gelangen die reduzierten Subtrahendenreihen auf 2 und die beiden unveränderten auf 8.

$M = 78\,217$	$78\,217$	$78\,217$
$- \quad 8$	392	128
$78\,209$	$77\,825$	$78\,089$
$- \quad 280$	$7\,800$	520
$77\,929$	$70\,025$	$77\,569$
$- \quad 680$	$17\,800$	920
$77\,249$	$52\,225$	$76\,649$
$- \quad 1\,080$	$27\,800$	$1\,320$
$76\,169$	$24\,425$	$75\,329$
$- \quad 1\,480$		$1\,720$
$74\,689$	$78\,217$	$73\,609$
$- \quad 1\,880$	$2\,592$	$2\,120$
$72\,809$	$275^2 = 75\,625$	$71\,489$
$- \quad 2\,280$	$12\,200$	$2\,520$
$70\,529$	$63\,425$	$68\,969$
$- \quad 2\,680$	$22\,200$	$2\,920$
$67\,849$	$41\,225$	$66\,049$
$- \quad 3\,080$	$32\,200$	$3\,320$
$64\,769$	$95^2 = \quad 9\,025$	$62\,729$
$- \quad 3\,480$		$3\,720$
$61\,289$		$59\,009$
$- \quad 3\,880$		$4\,120$
$57\,409$		$54\,889$
$- \quad 4\,280$		$4\,520$
$53\,129$		$50\,369$
$- \quad 4\,680$		$4\,920$
$48\,449$		$45\,449$
$- \quad 5\,080$		$5\,320$
$43\,369$		$40\,129$
$- \quad 5\,480$		$5\,720$
$37\,889$		$34\,409$
$- \quad 5\,880$		$6\,120$
$32\,009$		$28\,289$
$- \quad 6\,280$		$6\,520$
$25\,729$		$21\,769$
$- \quad 6\,680$		$6\,920$
$19\,049$		$14\,849$
$- \quad 7\,080$		$7\,320$
$11\,969$		$7\,529$
$- \quad 7\,480$		
$67^2 = \quad 4\,489$		

$$78\,217 = 67^2 + 2 \cdot 192^2 = 95^2 + 2 \cdot 186^2 = 275^2 + 2 \cdot 36^2.$$

Die 3 Brüche $\frac{67 \pm 95}{192 \pm 186}, \frac{95 \pm 275}{186 \pm 36}, \frac{67 \pm 275}{192 \pm 36}$ liefern die 3 Primteiler von M, nämlich:

$3^2 + 2 \cdot 2^2 = 17$, $5^2 + 2 \cdot 3^2 = 43$, $3^2 + 2 \cdot 7^2 = 107$; $78217 = 17 \cdot 43 \cdot 107$.

Spezialisationen der Hauptmethoden.

Den beiden Hauptmethoden schließen sich ihre Spezialisationen an. Da M sowohl eine lineare, als auch eine quadratische Form vorgeschrieben wird, läßt sich sowohl jene, als auch diese spezialisieren. Euler führt jenes in C 1, 26, dieses in C 1, 25 aus. Hier behandelt er die Form $x^2 + 1$, d. h. die Form (1, 0, 1), in der die eine Unbestimmte den konstanten Wert 1 behält. Sein Ziel ist, sämtliche Teiler einer solchen Form für einen gegebenen Wert von x zu bestimmen und damit die primen von den zusammengesetzten zu unterscheiden. Zunächst legt er die lineare Form der Wurzel x fest, falls $x^2 + 1$ durch die Primzahl p oder eine Potenz derselben geteilt wird. Aus (3) S. 23 folgt, daß p im besonderen Falle nur die 2, im allgemeinen nur von der Form $4n + 1$ sein kann. Da mithin jeder Teiler von $x^2 + 1$ gleich der Summe 2er Quadrate wird, so stellt man, $p = x_1^2 + y_1^2$ gesetzt, die Gleichung auf:

$$x^2 + 1 = (x_1^2 + y_1^2)\ (X^2 + Y^2) = (x_1 X \pm y_1 Y)_2 + x_1 Y \mp y_1 X)^2.$$

Nun substituiert man:

$$x_1 Y \mp y_1 X = \pm 1;\ x_1 X \pm y_1 Y = \pm x.$$

Euler löst die erste unbestimmte Gleichung mit Hilfe des Algorithmus zur Bestimmung des größten gemeinschaftlichen Teilers und desjenigen der Kettenbrüche (vgl. C 1, 25 S. 359 mit den Anmerkungen). x genügt hierauf den beiden Kongruenzen

$$x \equiv \pm (x_1 X + y_1 Y) \text{ mod. } p).$$

Es erhellt, daß p mit irgend einer seiner Potenzen vertauschbar ist. Es fehlt aber der Nachweis, daß nur 2, in ihrem konstanten Gliede entgegengesetzte Wurzelformen x bestehen, den die Theorie der quadratischen Reste liefert. Nach dieser besitzt die Kongruenz: $x^2 \equiv -1$ (mod. p^μ) nur 2, mod. p^μ inkongruente, einander entgegengesetzte Wurzeln. Jeder Primzahl p, bzw. ihrer Potenz p^μ, ordnen sich mithin 2 Wurzelformen $hp \pm \alpha$ zu, in die die Werte x aller durch p, bzw. p^μ, teilbaren Zahlen $x^2 + 1$

eingehen. Nimmt x_0 aus einer vorgegebenen Zahl $M = x_0^2 + 1$ mehrfach solche Wurzelformen an, so wird M durch sämtliche dazu gehörende Primzahlen, bezw. Primzahlpotenzen, geteilt. Euler begnügt sich nun nicht mit der Angabe der Methode und ihrer Verdeutlichung durch einige Beispiele, sondern er führt sie an allen Zahlen $M = x^2 + 1$ bis zu 2 250 000 durch. Eine erste Tabelle paart die beiden Wurzelformen mit den entsprechenden Primzahlen der Form $4n + 1$ bis zur Grenze 2000, ein Anhang dazu mit den entsprechenden niedrigsten Potenzen ihrer Anfangsglieder. Sie ermöglicht es, die Teiler aller M und weiter aller gleichformigen Zahlen bis zu 4 000 000 zu ermitteln. M setzt sich aus sovielen verschiedenen Primteilern zusammen, als sein x in den Wurzelformen der ersten Tabelle auftritt. Findet dies nirgends statt, so ist M sicherlich prim. Eine zweite Tabelle ordnet den Werten x, die bis zu 1500 ansteigen, alle unter ihnen liegenden Teiler der Zahlen x^2+1 zu; mithin führt sie die Faktorenbestimmung aller M aus. Diejenigen x, die sich bzw. nur mit den Teilern 1, 2, 5 und 10, mithin bzw. mit den Primzahlen x^2+1, $\frac{x^2+1}{2}$, $\frac{x^2+1}{5}$ und $\frac{x^2+1}{10}$ verbinden, werden gruppenweise in 4 kleineren Tafeln zusammengefaßt, von denen die erste noch die primen $x^2 + 1$ selber, darunter $112 > 100\,000$, $49 > 1\,000\,000$ aufführt. — Die nächste Abhandlung, C 1, 26, spezialisiert die lineare Form der zu untersuchenden Zahl M. M hat die lineare Hauptform $4n + 1$ und deswegen a priori die quadratische (1, 0, 1). Der Grundgedanke der Methode besteht nun darin, daß M noch lineare Nebenformen beigelegt werden, die ihrerseits lineare Formen der Unbestimmten x und y bedingen. Dadurch geht die Zahl der Subtrahendenquadrate, andrerseits aber auch der Bereich der der Methode zugänglichen M erheblich zurück; diese gewinnt an Kürze, verliert aber an Allgemeinheit.

1. M hat die beiden Nebenformen $3m + 2$ und $5m + 2$, mithin unter Hereinziehung der Hauptform die resultierende Form $60m + 17$. Diese bewirkt aber die Unbestimmtenformen:

$$15p \pm 1, 4, \text{ mithin } x \text{ und } y \equiv \pm 1, 4 \pmod{15}.$$

2. M hat die beiden Nebenformen: $3m + 2$ und $5m + 3$; demnach $M \equiv 2 \pmod 3 \equiv 3 \pmod 5 \equiv 1 \pmod 4$ oder $\equiv 53 \pmod{60}$, d. h. von der Form $60m + 53$. Daraus ent-

springt: x und $y \equiv \pm 2, 7 \pmod{15}$ oder für x und y die lineare Form $15p \pm 2, 7$.

3. Spezialisation der Hauptform für sich. $4n + 1$ schließt u. a. die 4 Formen in sich ein: α) $32m + 5$, β) $32m + 13$, γ) $32m + 21$ und δ) $32m + 29$. Damit vereinen sich folgende Unbestimmtenformen: mit (α) $x = 4p \pm 2$, $y = 16p \pm 1$, mit (β) $x = 4p \pm 2$, $y = 16p \pm 3$, mit (γ) $x = 4p \pm 2$, $y = 16p \pm 7$, mit (δ) $x = 4p \pm 2$, $y = 16p \pm 5$.

4a) Verknüpfung von (1) und (3). $M \equiv 17 \pmod{60}$, $\equiv 5, 13, 21, 29 \pmod{32}$, $x \equiv \pm 1, 4 \pmod{15}$, $\equiv \pm 2 \pmod{4}$, $y \equiv \pm 1, 4 \pmod{15}$, $\equiv \pm (1, 3, 7, 5) \pmod{16}$.

In allen 4 Fällen ergibt sich für die 1. Unbestimmte $x \equiv \pm (14, 26) \pmod{60}$ oder die Form $60p \pm (14, 26)$.

	M =	y =
1—3α:	480 m + 77;	240p ± (19, 29, 61, 109)
1—3β:	480 m + 197;	240p ± (1, 31, 49, 79)
1—3γ:	480 m + 317;	240p ± (11, 59, 91, 101)
1—3δ:	480 m + 437;	240p ± (41, 71, 89, 119)

b) Verbindung von (2) und (3).

$M \equiv 53 \pmod{60} \equiv 5, 13, 21, 29 \pmod{32}$.
$x \equiv \pm 2, 7 \pmod{15} \equiv \pm 2 \pmod{4}$
$y \equiv \pm 2, 7$ („) $\equiv \pm (1, 3, 7, 5) \pmod{16}$.

Wiederum in allen 4 Fällen x von derselben Form $60p \pm (2, 22)$; dagegen verschiedene Formen von M und y.

	M =	y =
2—3α:	480 m + 53;	240p ± (7, 23, 73, 103)
2—3β:	480 m + 173;	240p ± (13, 67, 77, 83)
2—3γ:	480 m + 293;	240p ± (17, 47, 97, 113)
2—3δ:	480 m + 413;	240p ± (37, 43, 53, 107)

(vgl. C 1, 26 S. 381 und 382). Die Formen von M vereinigen sich in (a) zu $120 m + 77$, in (b) zu $120 m + 53$. Auf alle Zahlen dieser Formen, aber auch nur auf diese, dehnt sich die spezialisierte Methode aus. Im übrigen deckt sich ihr Gang fast vollkommen mit dem der ersten Hauptmethode. Man ordnet M zunächst in eine der 8 obigen Formen unter und richtet dann entsprechend den 8 zugehörigen Formen von y eine achtfache Subtraktionskette ein, die aber allemal, zum Unterschiede von der Hauptmethode mit dem kleinstmöglichen Quadrate eingeleitet

wird. In jeder Kette erkennt man aufs neue Subtrahenden und Differenzen als arithmethische Progressionen 2. Ordnung und zwar mit der konstanten Differenz 115 200; die Entwicklung der Differenzenreihen zur Subtrahendenreihe teilt nämlich der zweiten von jenen konstante Glieder zu:

$$\begin{array}{llll} y^2 & (240 \pm y)^2 & (480 \pm y)^2 & (960 \pm y)^2 \\ 57\,600 \pm 480\,y & 3 \cdot 57\,600 \pm 480\,y & 5 \cdot 57\,600 \pm 480\,y & \\ & 115\,200 & 115\,200 & \end{array}$$

Man vermindert also M um das kleinste y^2, hierauf die Differenz $M - y^2$ um $57\,600 \pm 480\,y$, die letzte Differenz um $3 \cdot 57\,600 \pm 480\,y$ u. s. f., bis schließlich die nächste Subtraktion die Differenz unter $\frac{M}{2}$ hinabdrücken würde; diese unterbleibt, die Kette schließt mit der letztausgeführten Subtraktion. Die beiden Vorzeichen veranlassen 2 getrennte Subtraktionsfolgen, die aber in ihren Anfangssubtrahenden und -differenzen übereinstimmen und deren darauffolgende jeweils um $960\,k \cdot y$ auseinanderstehen, weshalb sie zusammengepaart und gewissermaßen in eine Kette verschmolzen werden. Liegt M unter einer Million, so sind nie mehr als 30 Subtraktionen erforderlich. Ein Beispiel möge die Methode näher erläutern:

$$M = 937\,037 = 1952 \cdot 480 + 77$$

Zum Abzug gelangen die Quadrate der 8 Reihen $y \equiv \pm (19, 29, 61, 109) \pmod{240}$.

$y \equiv \pm 19$		$y \equiv \pm 29$		$y \equiv \pm 61$		$y \equiv \pm 108$	
937 037	57 600	937 037	57 600	937 037	57 600	937 037	57 600
— 361	9 120	841	13 920	3 721	29 280	11 881	52 320
936 676	936 676	936 196	936 196	933 316	936 316	925 156	925 156
— 66 720	48 480	71 520	43 680	86 880	28 320	109 920	5 280
869 956	888 196	864 676	892 516	846 436	907 996	815 236	919 876
— 181 920	163 680	186 720	158 880	202 080	143 520	225 120	120 480
688 036	724 516	677 956	733 636	644 356	764 476	590 116	799 396
					258 720		235 680
					505 756		563 716

Da nirgendwo die Differenz quadratisch wird, kann M nicht prim sein, sondern muß einen nichtquadratischen Faktor m_2 (vgl. S. 27) einschließen. Tatsächlich ist

$$937\,037 = 31 \cdot 30\,227.$$

Ausdehnung der Eulerschen Methoden auf die Form (1, 0, 5)

Die Eulersche Methode läßt sich an den nächsteinfachen Formen (1, 0, 3) und (1, 0, 5) in ähnlicher Gestaltung wiederholen. Nach S. 15 und 16 werden a priori durch (1, 0, 3) alle ungeraden Zahlen der Form $3n + 1$; durch (1, 0, 5) alle solchen von den Formen $20n + 1$ und $20n + 9$; dagegen durch (2, 1, 3) diejenigen der Formen $20n + 3$ und $20n + 7$; durch keine der beiden quadratischen Formen schließlich diejenigen dargestellt, welche in keiner der 4 linearen Formen oder in den 4 andern $20n + 11$, $20n + 13$, $20n + 17$ und $20n + 19$ enthalten sind. Eine Zahl m der Formen $20n + 3, 7$ ist Nichtrest von 5 und -5; da 2 ebenfalls Nichtrest von -5 ist, ist $2m$ Rest von -5 und mithin durch (1, 0, 5) schlechthin darstellbar. Je nachdem also die zu prüfende Zahl M in die Formen $20n + 1, 9$ oder $20n + 3, 7$ eingeht, sucht man ihre Zerlegungen oder diejenigen ihres Doppelwertes durch (1, 0, 5). Ein Mißerfolg kündet die gänzliche oder teilweise Zusammensetzung von M aus Primteilern der 4 Formen $20n + 11, 13, 17, 19$ in nichtquadratischem Verband an; eine einzige eigentliche Zerlegung erweist M als prim oder primäquivalent, mehrere dagegen als aus verschiedenen Primteilern der 4 Formen $20n + 1, 3, 7, 9$ zusammengesetzt; uneigentliche Zerlegungen übermitteln Teiler der ersteren Zusammensetzung, aber in quadratischer Form. Nach Eulerschem Vorbild gibt nun die Form (1, 0, 5) den Schlüssel zu folgender Methode, die an Wirksamkeit jenem wohl kaum nachstehen dürfte. Genau soviel Zerlegungen M, bzw. 2 M, durch (1, 0, 5), genau soviel gestattet sein Doppelwert 2 M, bzw. 4 M durch (2, 0, 10). Diese letzteren, d. h. diejenigen in ein zweifaches und zehnfaches Quadrat, werden gefordert. Zu diesem Zwecke bemerkt man:

1) 2 M, bzw. 4 M, kommen die Formen $40n + 2$ und $40n + 18$, bzw. $80n + 12$ und $80n + 28$; mithin die beiden Endziffern 2 und 8 zu. Zieht man also die Doppelquadrate $2x^2$ ab, so wird man sich dabei, da die Differenz in einer 0 endigen muß, je nach der Endziffer von 2 M, bzw. 4 M, auf die Doppelquadrate mit der Endziffer 2 oder auf diejenigen mit der Endziffer 8 beschränken. Beide Arten zerfallen nach dem Einteilungsgrund gleicher Wurzelendziffer in 4 Reihen, von denen jede nach S. 31 eine arithmetische Reihe 2. Ordnung mit der konstanten Differenz 400 bildet; in den Doppelquadraten

auf 2 schließt x mit einer der Ziffern 1, 4, 6, 9; in denen auf 8 mit einer der Ziffern 2, 3, 7, 8.

2) Jede der 8 Reihen spaltet sich in 5 Unterreihen, in deren einzelner die vorletzte Ziffer gleichbleibt. Da x niemals auf 0 oder 5 ausgehen kann, so werden mit $2x^2$ nur $2(x+50)^2$, $2(x+2\cdot 50)^2$, $2(x+3\cdot 50)^2 \ldots 2(x+k\cdot 50)^2 \ldots$ das gleiche Endziffernpaar bewirken. Diese Doppelquadrate reihen sich aber zu einer arithmetischen Reihe 2. Ordnung mit dem Anfangsglied $200x + 5000$ ihrer 1. Differenzenreihe und der konstanten Differenz 10000 aneinander. Somit stimmen die 5 Unterreihen mit ihrer Oberreihe in ihrem Charakter überein. Da ferner die 1. Differenzenreihe der letzteren (vgl. S. 31) in ihren Gliedern stets eine gerade Anzahl von Zehnern enthält, so können in jeder Oberreihe je nach der vorletzten Ziffer ihres Anfangsgliedes vor die 2 oder 8 entweder nur die geraden oder nur die ungeraden Ziffern treten. Da die Differenz $10y^2 = M - 2x^2$ an ihre zweitletzte Stelle ebenfalls ausschließlich die geraden oder die ungeraden Ziffern zuläßt, worüber gleichfalls dieselbe Stelle ihres Anfangswertes entscheidet, von diesen aber beidemale 3 quadratisch und 2 nichtquadratisch sind $\binom{0,\,4,\,6\,—\,2,\,8}{1,\,5,\,9\,—\,3,\,7}$, so erkennt man, daß von den 5 Unterreihen jedesmal 2 wegen Untauglichkeit ausgeschlossen werden.

3) Wie die Subtrahenden, so schließen also auch die Differenzen jeder Unterreihe mit dem gleichen Ziffernpaar. Ist dieses eine Doppelnull oder 50, so können unter ihnen nur die reinen Tausender, bzw. Vierteltausender, zehnfache Quadrate darbieten. Die Reihe der Doppelquadrate, die solche Differenzen zustande bringt, ist, falls $2x_0^2$ ihr kleinstes Glied angibt:

$2x_0^2 \quad 2(x_0+250)^2 \quad 2(x_0+2\cdot 250)^2 \ldots \quad 2(x_0+k\cdot 250)^2$;

sie stellt sich mithin als arithmetische Progression 2. Ordnung mit dem Anfangsglied $1000x_0 + 125000$ und der konstanten Differenz 250000 dar. Die Unterreihe, in der die neue Teilreihe enthalten ist, geht damit auf diese zurück.

4) Gelangt $4M = 2x^2 + 10y^2$ zur Untersuchung, so müßte mit x auch y gerade und damit die rechte Seite jener Gleichung durch 8 teilbar werden, während es die linke nur durch 4 ist. Da somit ein gerades x widerlegt ist, genügt es, von 4M nur die sechs Unterreihen mit ungerader Wurzelendziffer abzuziehen, was einen Mehraufwand an rechnerischer Arbeit für die vierfache Zahl M beseitigt.

5) Das Verfahren wird nun dahin geleitet, daß man von dem doppelten M die **12**, von dem vierfachen M die 6 noch zulässigen Unterreihen hinwegnimmt. Kommt in 2M, bzw. 4M, Subtrahend und Differenz die Endziffer zum Fortfall, so muß die letztere ein reines Quadrat wiedergeben können. Soviel Mal dies eintritt, so viel Zerlegungen von M, bzw. 2M, in (1, 0, 5) haben statt. Nachstehend sind die 5 ersten Doppelquadrate jeder der 8 Oberreihen mit den zugehörigen Wurzelwerten und den 1. Differenzen derjenigen Unterreihen, deren Anfangsglieder sie sind, zusammengestellt.

a) Doppelquadrate auf **2**:

	x = 1	11	21
mit der Wurzelendziffer 1:	02 (5200),	242 (7200),	882 (9200),
	31	41	
	1922 (11200),	3362 (13200);	
	9	19	29
„ „ „ 9:	162 (6800),	722 (8800),	1682 (10800),
	39	49	
	3042 (12800),	4802 (14800);	
	4	14	24
„ „ „ 4:	32 (5800),	392 (7800),	1152 (9800),
	34	44	
	2312 (1188),	3872 (13800);	
	6	16	26
„ „ „ 6:	72 (6200),	512 (8200),	1352 (10200),
	36	46	
	2592 (12200),	4232 (14200);	

b) Doppelquadrate auf **8**:

	3	13	23
mit der Wurzelendziffer 3:	18 (5600),	338 (7600),	1058 (9600),
	33	43	
	2178 (11600),	3698 (13600);	
	7	17	27
„ „ „ 7:	98 (6400),	578 (8400),	1458 (10400),
	37	47	
	2738 (12400),	4418 (14400);	
	2	12	22
„ „ „ 2:	08 (5400),	288 (7400),	968 (9400),
	32	42	
	2048 (11400),	3528 (13400);	
	8	18	28
„ „ „ 8:	128 (6600)	648 (8600)	1568 (10600),
	38	48	
	2888 (12600),	4608 (14600).	

6) Die Methode soll an 3 Beispielen praktisch durchgeführt werden.

α) $M = 137209 = 20n + 9$

$2M = 274418$

27 441	27 441	27 441	27 441	27 441	27 441	27 441	27 441	27 441
8 241	105	217	57	145	0	352	12	460
19 200	27 336	27 224	27 384	27 296	27 441	27 089	27 429	26 981
	960	1 160	840	1 040	540	1 340	660	1 460
27 441	26 376	26 064	26 544	26 256	26 901	25 749	26 769	25 521
441	1 960	2 160	1 840	2 040	1 540	2 340	1 660	2 460
27 000	24 416	23 904	24 704	24 216	25 361	= 23 409	25 109	23 061
17 200	2 960	3 160	2 840	3 040	2 540	153^2 3 340	2 660	3 460
9 800	21 456	20 744	21 864	21 176	22 821	20 069	22 449	19 601
	3 960	4 160	3 840	4 040	3 540	4 340	3 660	4 460
27 441	17 496	16 584	18 024	17 136	19 281	15 729	18 789	15 141
5 916	4 960	5 160	4 840	5 040	4 540	5 340	4 660	5 460
21 525	12 536	11 424	13 184	12 096	14 741	10 389	14 129	9 681
	5 960	6 160	5 840	6 040	5 540	6 340	5 660	6 460
27 441	6 576	5 264	7 344	6 056	9 201	4 049	8 469	3 221
21 516			6 840		6 540		6 660	
5 925			504		2 661		1 809	

$2M = 2 \cdot 142^2 + 10 \cdot 153^2$; $M = 142^2 + 5 \cdot 153^2$,
mithin 137 209 prim.

β) $M = 70327 = 20n + 7$

$4M = 281308$

Subtrahiert werden nur Doppelquadrate ungerader Wurzelendziffer.

28 130	28 130	28 130	28 130	28 130
105	1	369	9	441
28 025	28 129	27 761	28 121	27 689
14 800	560	1 360	640	1 440
13 225	27 569	26 401	27 481	26 249
$= 115^2$	1 560	2 360	1 640	2 440
	26 009	24 041	25 841	23 809
	2 560	3 360	2 640	3 440
28 130	23 449	20 681	23 201	20 369
10 305	3 560	4 360	3 640	4 440
17 825	19 889	16 329	19 561	15 929
	4 560	5 360	4 640	5 440
	15 329	10 969	14 921	10 489
	5 560	6 360	5 640	6 440
	9 769	4 609	9 281	4 049
	6 560		6 640	
	3 209		2 641	

$4M = 2 \cdot 273^2 + 10 \cdot 115^2$,
$2M = 273^2 + 5 \cdot 115^2$; 70 327 prim.

γ) $M = 502\,661 = 20\,n + 1$

$M = 1005\,322$

100 532	100 532	100 532	100 532	100 532	100 532	100 532	100 532	100 532
3 432	88	336	16	168	3	231	51	423
97 100	100 444	100 196	100 516	100 364	100 529	100 301	100 481	100 109
17 600	920	1 320	680	1 080	580	1 180	820	1 420
79 500	99 524	98 876	99 836	99 284	99 949	99 121	99 661	98 689
42 600	1 920	2 320	1 680	2 080	1 580	2 180	1 820	2 420
36 900	97 604	96 556	98 156	97 204	98 369	96 941	97 841	96 269
	2 920	3 320	2 680	3 080	2 580	3 180	2 820	3 420
100 532	94 684	93 236	95 476	94 124	95 789	93 761	95 021	92 849
2 832	3 920	4 320	3 680	4 080	3 580	4 180	3 820	4 420
97 700	90 764	88 916	91 796	90 044	92 209	89 581	91 201	88 429
16 400	4 920	5 320	4 680	5 080	4 580	5 180	4 820	5 420
81 300	85 844	83 596	87 116	84 964	87 629	84 401	86 381	83 009
41 400	5 920	6 320	5 680	6 080	5 580	6 180	5 820	6 420
39 900	79 924	77 276	81 436	78 884	82 049	78 221	80 561	76 589
	6 920	7 320	6 680	7 080	6 580	7 180	6 820	7 420
100 532	73 004	69 956	74 756	71 804	75 469	71 041	73 741	†69 169
11 907	7 920	8 320	7 680	8 080	7 580	8 180	7 820	8 420
88 625	65 084	61 636	67 076	63 724	67 889	62 861	65 921	60 749
36 900	8 920	9 320	8 680	9 080	8 580	9 180	8 820	9 420
51 725	56 164	52 316	58 396	54 644	59 309	53 681	57 101	51 329
	9 920	10 320	9 680	10 080	9 580	10 180	9 820	10 420
100 532	46 244	41 996	48 716	44 564	*49 729	43 501	47 281	40 909
7	10 920	11 320	10 680	11 080	10 580	11 180	10 820	11 420
100 525	35 324	30 676	38 036	33 484	39 149	32 321	36 461	29 489
13 100	11 920	12 320	11 680	12 080	11 580	12 180	11 820	12 420
87 425	23 404	18 356	26 356	21 404	27 569	20 141	24 641	17 069
38 100	12 920	13 320	12 680	13 080	12 580	13 180	12 820	13 420
49 325	10 484	5 036	13 676	8 324	14 989	6 961	11 821	3 649
					13 580			
					1 409			

$*49\,729 = 223^2$, $\dagger 69\,169 = 263^2$

$M = 504^2 + 5 \cdot 223^2 = 396^2 + 5 \cdot 263^2$

Die Teiler von M entstehen daraus nach S. 22.

$$\frac{504 + 396}{223 - 263} = -\frac{900}{40} = -\frac{45}{2} = \frac{p}{q}$$

$$\frac{45 \cdot 45}{5 \cdot 2^2} = \frac{405}{4} = \frac{p'}{q'};\quad 449 = p' + q'$$

$$\frac{504 + 396}{223 + 263} = \frac{900}{486} = \frac{50}{27} = \frac{p}{q};$$

$$\frac{50 \cdot 50}{5 \cdot 27^2} = \frac{50 \cdot 10}{27^2} = \frac{p'}{q'}.\quad 1229 = p' + q'.$$

$$502\,661 = 449 \cdot 1229.$$

Eulers Satz über die kongruenten Formen.

Nachdem die einfachen Formen (1, 0, 1), (1, 0, 2), (1, 0, 3) und (1, 0, 5) eine große Fruchtbarkeit in der Primzahlbestimmung enthüllt haben, liegt die Frage nahe, ob jene den Komplex derartiger Formen erschöpfen oder ob dieser noch andere, ähnlich wirkende und wieviele derselben umfaßt. Der große Vorteil, den jene 4 Formen gewähren, besteht darin, daß sie jede prime oder primäquivalente Zahl, die in die zugehörigen Linearformen eingeht, einmalig, dagegen eine zusammengesetzte Zahl letzterer Beschaffenheit, wenn überhaupt, mehrmalig zerlegen müssen. Teilt nun die allgemeine Form (a, o, c) mit ihnen diese Eigenschaft? Euler greift dieses Problem in C 2, 59—63 an und entdeckt, daß nur eine beschränkte Anzahl von Formen den 4 einfachsten an die Seite gestellt werden können. Die Produkte ihrer Außenglieder stellen stets dieselben 65 Zahlen dar, die sich folgender aufsteigender Reihe einfügen: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848. Diese 65 Zahlen bezeichnet Euler als kongruent (numeri congrui vel idonei); die Formen, deren Außenglieder ihre relativ primen Faktoren sind, als kongruente Formen (formae congruae). Alle andern unzählig vielen Formen, die sich nicht dem Gesetz der mehrmaligen Wiedergabe zusammengesetzter Zahlen unterwerfen, treten den ersteren als inkongruente Formen gegenüber. Wie haben sich nun Euler die 65 kongruenten Zahlen erschlossen? Ihre Kenntnis schöpft er aus folgender Regel:

Eine Zahl Δ ist kongruent oder inkongruent, je nachdem sämtliche Summen $s = x^2 + \Delta < 4\Delta$, mit relativ primen Summanden, prime und primäquivalente oder auch eine oder einige zusammengesetzte Werte annehmen. Als primäquivalent gelten dabei die Doppelwerte und Quadrate der Primzahlen, sowie sämtliche Potenzen der 2.

Die Beweise Eulers für seinen Satz.

Auf diese Regel führt ihn folgender Hilfssatz: Zerlegt eine Form (a, o, c) eine zusammengesetzte Zahl nur auf eine einzige Weise, so gibt es noch unendlich viele andere zusammen-

gesetzte Zahlen, auf die sie in gleicher Weise wirkt. In jeder zerlegenden Form werden von nun an Koeffizienten und Unbestimmte unter sich und jede der letzteren prim zum Koeffizienten der andern festgesetzt. Sieht man von seinem ersten Beweise jenes Satzes (vgl. C 2, 59, S. 202), der seine Beweiskraft durch dreifache Spezialisation völlig einbüßt, ab, so birgt der andere (vgl. S. 205) folgende Schlußreihe. Voraussetzung ist, daß eine zusammengesetzte Zahl M, der rücksichtlich des Endzieles von vorneherein die Form (1, 0, ac) zugeschrieben wird, nur einmal in diese Form eingeht. Spaltet man nun M in zwei Faktoren M_1 und M_2, so folgt aus Satz (4) S. 24, daß keiner der beiden die Formen (1, 0, ac) und (a, o, c) annehmen kann. Denn räumt man dies dem einen ein, so spricht man es nach (4) auch dem andern und damit M nach Satz (1) S. 20 eine doppelte Zerlegung durch (1, 0, ac) zu, was der Voraussetzung entgegensteht. Es zeigt sich weiterhin, daß jeder der beiden Faktoren die Form (a, o, c) unendlich vielmal teilt. Weist man dies für den kleineren, welchen M_2 angeben möge, nach, so substituiert man: $x = kx_0 + g_1 \cdot M_2$, $y = k \cdot y_0 + g_2 \cdot M_2$ und findet:

$$(kx_0 + g_1 \cdot M_2)^2 + ac\,(ky_0 + g_2 \cdot M_2)^2 = M_2\,[k^2 \cdot M_1 + M_2\,(g_1^2 + acg_2^2) + 2k\,(g_1 x_0 + acg_2 \cdot y_0)],$$

oder wenn M_3 den Wert der eckigen Klammer bedeutet, $= M_2 \cdot M_3$. Euler schließt nun, daß $M_2 \cdot M_3$ auch nur einmalig in (1, 0, ac) enthalten ist, und hält damit seinen Satz mit Rücksicht auf die unendlich vielen Werte, die den 3 Hilfsgrößen k, g_1 und g_2 offenstehen, für erwiesen. Unter der unendlichen Mannigfaltigkeit der Produkte $M_2 \cdot M_3$ findet sich nun eines, das unter 4ac liegt. Denn in M_3 kann über k_1 g_1 und g_2 dermaßen verfügt werden, daß $M_3 < M_2$ mithin $M_2 \cdot M_3 < M_1 M_2$ wird. Durch Wiederholung der obigen Substitution und passende Wahl des neuen Tripels von Hilfszahlen gelangt man zu einem noch kleineren Produkte $M_3 \cdot M_4$, das wiederum auf ein unter ihm stehendes führt u. s. f. Zuletzt wird das oben genannte Produkt dem Algorithmus sein Ende setzen. Euler glaubt nun gezeigt zu haben, daß, falls eine beliebige, zusammengesetzte Zahl auf einzige Weise durch (1, 0, ac) zerlegt wird, dies auch von einer solchen $< 4ac$ gilt. Ohne weiteres dehnt er den Hilfssatz auf alle Formen aus, deren Außengliederprodukt = ac ist; enthält also eine solche Form eine zusammengesetzte Zahl nur einmal, so enthalten sie alle unzählig viele zusammengesetzte Zahlen ebenfalls bloß ein-

mal, vor allem die Form (1, 0, ac) eine solche $< 4ac$. Auf dieses Ergebnis baut Euler sein Kriterium auf. Jedoch hat er es damit auf eine keineswegs streng theoretische Grundlage gestellt, vielmehr ist er ausschließlich durch Induktion auf den richtigen Pfad geleitet worden, wie denn seine Theorie sich an Beispiele festklammert; sie umrankt, anstatt sie beherrscht; mit vertauschter Rolle zu ihrer Erläuterung dient. Ihre Mängel erkennt man in folgenden: 1. Da Satz (4) einen primen Faktor von M in gleicher oder in der Form (a, o, c) voraussetzt, so müßten alle Faktoren M_1, M_2, M_3 . . . . prim sein. 2. Obwohl das Produkt $M = M_1 \cdot M_2$ nur eine Zerlegung durch (1, 0, ac) gestattet, und seine Faktoren M_1 und M_2 weder in die gleiche (1, 0, ac), noch in irgend eine andere mit dem Außengliederprodukt ac eingehen können, folgt noch nicht, daß das aus M_1 M_2 hervorgehende, nächstkleinere Produkt $M_2 \cdot M_3$ nur einmal in (1, 0, ac) enthalten sein kann. Eine mehrmalige Zerlegung desselben würde nach Satz (3) S. 22 M_2 keine der obigen Formen unbedingt vorschreiben. Kein Produkt der ganzen Kette bis zum kleinsten ist also an ein einziges Eingehen in (1, 0, ac) gebunden. 3. Es fehlt der Nachweis, wie die 3 Größen k, g_1 und g_2 angenommen werden müssen, damit $M_2 \cdot M_3$ unter $M_1 \cdot M_2$ sinkt. 4. Man vermißt den theoretischen Beleg dafür, daß das kleinste Glied der Kette $M_1 \cdot M_2$, $M_2 \cdot M_3$ . . . . $< 4ac$ ist, womit das Kriterium seinen Grund und Boden verliert. 5. Was berechtigt Euler zur Verallgemeinerung seines Hilfssatzes (vgl. oben)? 6. Worauf stützt er seine Primäquivalenz? —

Beweis des Eulerschen Satzes durch die Gaußsche Formentheorie.

a) Die 65 in ihren eigentlich primitiven Geschlechtern einklassigen Determinanten sind sicherlich kongruent.

Die unantastbare, „streng geometrische“ Begründung des Eulerschen Kriteriums erfolgt erst durch die Gaußsche Theorie der quadratischen Formen. Sie läßt sich an einer Einzelform überhaupt nicht durchführen. Eulers Weg verkehrt sich in den entgegengesetzten. Der Beweis hält sich nicht an eine unveränderliche, sondern an eine Gruppe unzählig vieler Formen, nämlich an diejenigen einer und derselben Determinante $D = b^2 - ac$, Eulers Hilfssatz wird durch die Eigenschaften der

Äquivalenz und der darauf gestützten Klassen der Formen von D ersetzt. Zu jeder Determinante D gehört eine endliche Anzahl reduzierter Formen (vgl. D. A. Art. 183 ff.). Ist $D > o$, so sind mehrere derselben untereinander äquivalent; jede solche Gruppe besteht aus einer Periode benachbarter Formen. Ist $D < o$, so kann eine reduzierte Form nur ihrer entgegengesetzten äquivalent sein. Jeder reduzierten Form, bzw. Formenpaar oder -periode sind aber unendlich viele Formen derselben Determinante äquivalent. Jene schließt man mit diesen in eine Formenklasse zusammen. Der 3. Fall $D = 0$ kann, da er den Eulerschen Entwicklungen fremd gegenübersteht, übergangen werden. Jede Determinante D enthält also ebensoviele Formenklassen, als sie, wenn $> o$, Perioden reduzierter Formen, wenn $< o$, reduzierte Formen, bzw. Formenpaare bestimmt. Im letzteren Falle heißt die Klasse, welcher 2 reduzierte Formen angehören, ambig (classis anceps nach Gauß). Weiterhin faßt man die Klassen in Geschlechter, deren Zahl stets einer Potenz der 2 gleichkommt, diese in Ordnungen zusammen. Als wichtigste Ordnung tritt die eigentlich primitive mit den eigentlich primitiven Geschlechtern und Klassen hervor; sie enthält sämtliche eigentlich primitiven Formen der Determinante D. In D. A. Art. 252 beweist Gauß, daß die Geschlechter derselben Ordnung gleich viel Klassen zählen. Die Menge κ derselben ist aber in derselben Determinante von Ordnung zu Ordnung und dann auch in den verschiedenen Determinanten ungleich. Erst Dirichlet gelang es, den funktionalen Zusammenhang zwischen κ und D aufzudecken (vgl. seine Recherches sur diverses appl...). Es gibt nun wenigstens 65 negative Determinanten D_1, die in ihren eigentlich primitiven Ordnungen sich durch das Minimum $\kappa = 1$ auszeichnen, die also in ihren eigentlich primitiven Geschlechtern nur je eine Klasse enthalten. Abgesehen vom Vorzeichen fallen sie vollkommen mit den 65 kongruenten Zahlen Eulers zusammen. Was bewirkt nun diese Beschränkung? Eine Zahl M, welche den quadratischen Rest D besitzt, wird durch alle Formenklassen von D dargestellt, in welche die Formen

$$(M, n_1, m_1), (M_1 - n_1, m_1), (M, n_2, m_2), (M, -n_2, m_2) \ldots\ldots$$
$$(M, n_m, m_m), (M, -n_m, m_m)$$

gehören, falls die Mittelglieder n und die Hinterglieder m die Bedeutung von S. 14 bewahren. Ist M prim zu 2D, so gestattet M nur einem einzigen eigentlich primitiven Geschlechte Dar-

stellungen; umfaßt dieses nur eine einzige Klasse, so geht der Darstellungsbereich von M auf diese zurück, die gesamten Formen (M, n, m) müssen sich in diese einreihen. Jede Form f_1, deren Determinante mit einer der D_1 übereinstimmt, muß eine zu $2D_1$ prime Zahl M soviel Mal darstellen, als die quadratische Kongruenz $(A_1)x^2 \equiv D_1 \pmod{M}$ inkongruente Wurzeln besitzt. Setzt sich M aus μ Primteilern zusammen, so ist die Wurzelzahl von $(A_1) = 2^\mu$ (vgl. S. 13). Verliert f_1 ihr Mittelglied, so vereinigen sich je **2** Darstellungen von M zu einer Zerlegung von M in 2 Vielfache von Quadraten (vgl. S. 12). Je nachdem also M einerseits eine Primzahl oder die Potenz einer solchen, andrerseits das Produkt aus mehreren der letzteren ist, wird M einmalig oder mehrmalig durch f_1 zerlegt. Damit ist der Schleier über den 65 kongruenten Zahlen gelüftet, mit andern Worten der Eulersche Satz bestätigt worden: Geht eine Zahl M in eine Form (a, o, c), deren Außenglieder sich zu einer kongruenten Zahl multiplizieren, nur einmalig ein, dann ist sie eine Primzahl oder die Potenz einer solchen; findet jenes aber mehrmalig statt, dann ist M als aus verschiedenen Primteilern zusammengesetzt charakterisiert. An M muß die Bedingung gestellt werden, daß es prim zu 2ac ist, welcher sich Euler in der Erwägung enthebt, daß die in Betracht gezogenen Zahlen M sie ohne weiteres einhalten. (Zum Beweise vgl. Meyer, Beweis eines von Euler entdeckten Satzes ... In.-Diss. Straßb. 1906).

Auf welche Gründe führt man nun das eigentliche Kriterium zurück, das Euler die kongruenten Zahlen übermittelt hat? Zunächst erhellt, daß alle D_1 ihnen angehören müssen. Allgemein wird eine zur Determinante prime Zahl M, je nachdem sie ungerade oder gerade ist, nur durch die eigentlich primitive Ordnung von D oder durch diese und durch die uneigentlich primitive Ordnung dargestellt. Letztere besteht aber nur dann, falls D die Form $4n+1$ hat. Kommt D also in den 3 anderen Formen bezüglich des Modulus 4 vor: $4n$, $4n+2$ und $4n+3$, so wird sich die Darstellung von M nur auf eigentlich primitive Formenklassen beschränken, und zwar werden sich so viele daran beteiligen, als die Kongruenz (A) (mod. M) inkongruente Wurzeln befriedigen. Erfolgt dies durch ihre Mindestzahl, was nach S. 13 ausschließlich für ein primes oder primäquivalentes M eintritt, so erfährt M nur durch ein Paar entgegengesetzter Formenklassen,

bzw. durch eine ambige Klasse Darstellungen. Da ein ungerades M den Totalcharakter eines Geschlechtes, ein gerades M aber die Spezialcharaktere sämtlicher Primteiler eines ungeraden D angibt, 2 verschiedene Geschlechter eines solchen D aber in diesen nicht übereinstimmen können, so folgt, daß die Klassen, welche an der Darstellung von M Teil haben, einem einzigen eigentlich primitiven Geschlecht angehören.

Nun bemerkt man, daß 1. die Summen $s = x^2 + \Delta$ (vgl. S. 45) mit denjenigen, zu $D = -\Delta$ primen Zahlen zusammenfallen, die in der Hauptform $(1, 0, \Delta)$ der Determinante D in dem Ausschnitt Δ bis 4Δ enthalten sind; 2. daß unter den 65 D_1 bloß 3, nämlich $D_1 = -3, -7, -15$ die Form $4n + 1$ haben, während die übrigen sich auf die 3 anderen Formen $4n + 0, 2, 3$ verteilen. Abgesehen von jenen, erkennt man in diesen vom theoretischen Gesichtspunkte aus kongruente Zahlen. Käme nämlich ein zusammengesetzter Wert s_1 vor, so fände eine mehrmalige Darstellung desselben durch das Hauptgeschlecht, folglich durch die Hauptklasse und damit durch die Hauptform statt. Da aber $y = 1$ und damit unveränderlich bleibt, ist auch diese ausgeschlossen.

Die Einschränkung der auf S. 45 festgesetzten Primäquivalenz auf die einfachen, doppelten und quadratischen Werte der ungeraden Primzahlen beruht auf der Unfähigkeit der Hauptformen $(1, 0, \Delta_1)$, ihre doppelten Quadrate und ihre einfachen und doppelten höheren Potenzen zur Darstellung zu bringen. Diese geht aus Schlüssen hervor.

1) s_1^2 überragt stets, ohne Rücksicht auf $\Delta_1 = 1$, das ohne weiteres als kongruente Zahl gewertet wird, die Grenze $4D_1$.

2) Das Quadrat einer zu $2D_1$ primen Zahl, das den Totalcharakter des Hauptgeschlechts aufzeigt, kann nur durch dieses dargestellt werden; ebenso jede Potenz einer solchen Zahl, falls nur irgend eine durch das Hauptgeschlecht dargestellt wird. Ginge nunmehr in $(1, 0, \Delta_1)$ $p^{2\kappa}$ oder $p^{2\kappa-1}$ ein, wo p eine ungerade Primzahl und $\kappa \geq 2$ ist, so müßte dies auch nach (2) für jede gerade Wurzel, bzw. für die Basis p zutreffen, was nach (1) unmöglich ist. Enthielte $(1, 0, \Delta_1)$ $2 \cdot p^{2\kappa}$ oder $2 \cdot p^{2\kappa+1}$ $(\kappa \geq 1)$ in der Weise, daß

$$2 \cdot p^{2\kappa(+1)} = x^2 + \Delta_1$$

wäre, so müßte Δ_1 nach der Eulerschen Voraussetzung über die Summennatur s notwendig ungerade sein. Da ferner 2, bzw. 2p Rest aller Primteiler von Δ_1 wäre, diesem aber die

uneigentlich primitive Ordnung fehlt, so müßten auch jene Zahlen, die auf jeden Fall unter die Quadratwurzel aus $2p^{2\kappa(+1)}$ hinabgehen, durch die Hauptform eine Darstellung finden, was gleichfalls gegen (1) verstößt.

Schließlich ergibt sich, daß keine Hauptform $(1, 0, \Delta_1)$, in der $\Delta_1 \not\equiv 3 \pmod 4$ ist, eine Potenz der 2 enthalten kann, da diese gerade die ausgeschlossene Form von D_1 bedingen würde. Deswegen kommt den 3 ersten Determinanten, deren entgegengesetzte Werte $\Delta_1 = 3, 7, 15 \equiv 3 \pmod 4$ sind, jene Eigenschaft zu; sie werden nämlich durch die Einheit bzw. zu den aufeinanderfolgenden Potenzen 4, 8, 16 der 2; 7 noch durch 3^2 zu 16 ergänzt. Man übersieht sofort, daß sie sich auch sonst wie kongruente Zahlen verhalten. Die Ausdehnung der Primäquivalenz auf die Potenzen der 2 rührt daher, daß, obwohl die Kongruenz $x^2 \equiv D \pmod{2^\kappa}$ 4 Wurzeln, nämlich $\pm r$, $\pm r + 2^{\kappa-1}$, besitzt, notwendig die Hälfte derselben auf die uneigentlich primitive Ordnung entfällt. Nebenbei erwähnt ist $D_1 = -3$ die einzige negative Determinante von der Form $8n + 5$ mit einklassig eigentlich primitiven Geschlechtern. Gauß beweist nämlich (D. A. Art. 256, VI), daß die Anzahl der Klassen sowohl in den eigentlich primitiven, als auch in den andern Geschlechtern aller übrigen gleichformigen negativen Determinanten stets durch 3 teilbar ist. Sie müssen schon aus dem Grunde aus der Reihe der D_1 heraustreten, weil ihre uneigentlich primitiven Ordnungen keine durch 4 teilbaren Zahlen aufnehmen, mithin eine solche $< 4\Delta_1$ und in der Summenform s_1 einbegriffen durch die Hauptform von D_1 mehrmals wiedergegeben werden müßte.

b) Können auch mehrklassige Determinanten kongruent sein?

Wenn nun sämtliche Δ_1 als kongruente Zahlen hervorgehen müssen, so frägt es sich, ob sich der Kongruenzbereich nicht auch auf Determinanten mit mehrklassigen primitiven Geschlechtern erstreckt. Die Entscheidung hierüber kann sofort gefällt werden, sobald jene sich auf Primzahlen und deren Quadrate beschränken. Die Summen s liefern nämlich im Bereiche Δ bis $\frac{4}{3}\Delta$ alle eigentlich primitiven reduzierten Formen von D mit zu D primem Mittelgliede b (vgl. D. A. Art. 174). Ist D nun eine kongruente Zahl, so können aus den s, wie

leicht ersichtlich, nur ambige Formen (2, 1, p), (p, b, p) entstehen; setzt man ferner D als mehrklassig voraus, so müßten sich jene mit mindestens ebensovielen nichtambigen reduzierten Formen paaren, welche aus den Summen s′ desselben Intervalles, deren Summanden in Teilergemeinschaft ständen, hervorgehen würden. Legt man aber schließlich D obige Beschränkung auf, so läßt die Ungleichung

$$2b \leqq a \leqq c$$

kein s′ zu. Eine mehrklassige Determinante p oder p^2 (p ungerade Primzahl) weist also die Eigenschaft der Kongruenz ab. Ist D beliebig zusammengesetzt, so weist sich D als inkongruent aus, wofern nur eine primitive reduzierte Form von D besteht, deren Mittelglied prim zu D. und deren Außengliederprodukt nicht primäquivalent ist. Letztere Forderung scheint fast durchgängig erfüllt zu sein; unter den kleinsten mehrklassigen D entziehen sich ihr nur die Determinanten:

36 (1, 0, 36) (4, 0, 9) (5, ±2, 8)
52 (1, 0, 52) (4, 0, 13) (7, ±2, 8)
66 (1, 0, 66) (2, 0, 33) (3, 0, 22) (6, 0, 11) 5, ±2, 14) (7, ±2, 10)
96 (1, 0, 96) (3, 0, 32) (4, 2, 25) (11, 4, 11) (5, ±2, 20) (7, ±3, 15)
100 (1, 0, 100) (4, 0, 25) (8, ±2, 13),

die sich aber in dem Intervalle $\frac{4}{3}\Delta$ bis 4Δ als inkongruent herausstellen. Der strenge Beweis ihrer jedesmaligen Verwirklichung jedoch liegt nicht ohne weiteres auf der Hand. Immerhin steht jedem mehrklassigen D die Möglichkeit offen, zusammengesetzte Zahlen $< 4\Delta$, die den Totalcharakter von D tragen, durch die Hauptform darzustellen; daran können sich doch noch sämtliche Klassen des Hauptgeschlechtes beteiligen.

Abgesehen von ihrem Determinantencharakter lassen sich unzählig viele Zahlengattungen als inkongruent erkennen. Zuvörderst sind es alle Zahlen von der Form $4n + 3$ mit Ausnahme von 3, 7 u. 15. Denn fügt man zu ihnen die zu ihnen primen ungeraden Quadrate hinzu, so werden alle diese Summen, mithin auch diejenigen $< 4\Delta$, durch 4 teilbar. In dem Intervalle Δ bis 4Δ können sich nur 2 Potenzen der 2 finden. Gibt $\Delta + 1$ eine solche, so ist die nächstfolgende $= \Delta + \Delta + 2$. Fiele sie mit einer Summe s zusammen, so müßte $\Delta + 2$ ein Quadrat sein und einer Potenz der 2 unmittelbar nachfolgen.

Mithin wäre

$$\Delta + 2 = x^2 = 1 + 2^\kappa \text{ oder } x^2 \equiv 1 \text{ (mod. } 2^\kappa).$$

Da die Wurzeln dieser Kongruenz ± 1, $\pm 1 + 2^{\kappa-1}$ sind, müßte

$$x^2 = 1 + 2^\kappa = 2^{2\kappa-2} \pm 2^x + 1,$$

mithin, da nur das untere Vorzeichen gelten kann,

$$2^{\kappa+1} = 2^{2\kappa-2}$$

werden, was den Exponenten $\kappa = 3$ bedingt. 9 ist also die einzige, auf eine Potenz der 2 folgende Quadratzahl. Läßt man demnach die vorweg angeführten 3 Werte außer acht, so ergibt sich, daß, falls unter $\sqrt{3\Delta}$ sich außer der 1 noch eine andere, zu 2Δ prime Zahl vorfindet, Δ mit Notwendigkeit eine inkongruente Zahl ist. Die Wahrung der letzten Bedingung mag ohne strengen Beweis hingenommen werden.

Ferner schließen sich alle Zahlen von den kongruenten aus, die einer zusammengesetzten Zahl vorhergehen; zu ihnen zählen u. a. alle Zahlen mit der Endziffer 9 ausschließlich der ersten. Ihnen treten weiterhin alle Zahlen Δ zur Seite, deren entgegengesetzte Werte D der Kongruenz genügen:

$$(A') \; x^2 \equiv D \text{ (mod. } p),$$

in der p eine ungerade, in Δ nicht aufgehende Primzahl $< 2\sqrt{\frac{\Delta}{3}}$ bedeutet. Diese Einschränkung bewirkt, daß $s = x^2 + \Delta$ niemals primäquivalent wird. Je nachdem also p von der Form $4n+1$ oder $4n+3$ ist, werden alle Zahlen $\Delta > \frac{3}{4}p^2$ zu den inkongruenten gestellt, die in die Restformen $c \cdot p + r$ oder in die Nichtrestformen $c \cdot p + n$ von p eingehen. Euler hat schon in C 2, 59 S. 211 diese ausschließenden Formen für die ersten Primzahlen bis 29 zusammengestellt. Jedoch wiederholt man dabei die Voraussetzung, daß, wenn bei unveränderlichem D p die ihm offenstehenden Primwerte durchläuft, die Wurzel x von (A') einmal prim zu D wird. Verläßt man diese besonderen Fälle, so muß der allgemeine Grund für die Verschiedenheit von kongruenten und inkongruenten Zahlen in der Verteilung der Primzahlen in Δ selber und seiner Nachbarschaft gesucht werden. Ist x durchweg ungerade und Δ kongruent und a) von der Form $4n$, b) von der Form $4n + 1$, c) von der Form $4n + 2$, so müssen

a) alle s einfache oder quadrierte Primzahlen, b) alle $\frac{s}{2}$ Primzahlen, c) alle s lauter einfache Primzahlen darstellen. Bislang fehlt der Nachweis, daß es nur 65 kongruente Zahlen gibt.

Eulers Sätze über die kongruenten Zahlen.

Über diese stellt Euler eine Reihe von Sätzen auf (C 2, 63), die er aber nur auf induktive Gewißheit gründet und die dasjenige entbehren, was Gauß geometrische Strenge nennt. Unter ihnen seien hervorgehoben: 1. Die kongruenten Zahlen enthalten nur die Quadrate 1, 4, 9, 16 und 25. 2. Je nachdem eine kongruente Zahl von der Form $4n + 3$ oder $4n + 1$ ist, ist ihr 4faches wieder eine solche oder nicht. 3. Hat eine kongruente Zahl die Form $4n + 2$, so ist $4(4n + 2)$ eine gleiche Zahl. In einem Anhange zu seiner Arbeit (C 2, 64) hebt Euler die merkwürdige Tatsache hervor, daß die Reihe der Δ_1 in jenen Thesen ein gewisses gesetzmäßiges Verhalten bekundet und trotzdem sich nicht ins Unendliche erstreckt, sondern nach 65 Gliedern abbricht, wie dies insofern als Gewißheit hingenommen werden könne, als bis zu 10 000 kein einziges Δ_1 mehr auftauche; eine Tatsache, die ihm im Gesamtgebiete seiner Forschungen noch niemals begegnet wäre und für die er deshalb nur den Ausdruck Paradoxon hat.

Anwendung der Eulerschen Methode auf alle kongruenten Formen.

Um nun wieder zum eigentlichen Gegenstande zurückzukehren, zieht Euler nicht nur die kongruenten Formen mit kleinstem Δ_1, sondern auch diejenigen mit größerem und größten Δ_1 zur Primzahlbestimmung heran. Die Methode bleibt in ihren Grundzügen ungeändert. Ein Unterschied gegen früher tritt nur dadurch hervor, daß die linearen Formen, die alle Zahlen von einer quadratischen kongruenten Form annehmen, fehlen. Da Euler das Reziprozitätsgesetz der quadratischen Reste wohl zuerst erkannt (vgl. Bachmann, El. d. Zahlenth. S. 124), dagegen nur induktiv und keineswegs streng begründet hat, überhaupt nicht bis zu seiner praktischen Verwendbarkeit durchgedrungen ist, so mußten sich ihm die linearen Teilerformen von $x^2 + \Delta_1$ (vgl. D. A. Art. 147—150) oder von $t^2 + \Delta_1 u^2$ (vgl. Leg. Théor. des nombres S. 261 u. ff.), die sich aus dem Rezi-

prozitätsgesetz herleiten und die er allerdings gekannt hat (vgl. C 2, 55), als ein zu fernes und unausgebautes Hilfsmittel verschließen. Er setzt demnach keine lineare Form der zu untersuchenden Zahl M voraus und sucht nicht ihre Zerlegung durch die jener entsprechende quadratische Form, sondern er legt gleich eine solche Form von M zugrunde. Da in die Teilerformen einer Determinante D die Hälfte aller ganzen Zahlen, in eine quadratische Form von D aber ein beschränkterer Teil derselben eingeht, so setzt die geänderte Voraussetzung die Brauchbarkeit der Methode erheblich herunter. Eine einmalige Zerlegung von M in eine kongruente Form f_1 wird also vorweggenommen. Liefert die Methode keine andere mehr, so muß M nach dem Eulerschen Satz über die kongruenten Formen (vgl. S. 45) eine Primzahl oder die Potenz einer solchen sein; im entgegengesetzten Falle ist M aus verschiedenen Primteilern zusammengesetzt, welche sich nach Satz (3) von S. 22 ermitteln lassen. Jede Eulersche Methode, die in ihrer Ausführung je nach der ihr unterworfenen Form f_1 von den andern abweicht, spiegelt denselben Grundtypus wieder: Der unveränderliche Minuend ist nicht M selber, sondern eines der Quadrate der gegebenen Zerlegung, Subtrahend S ist eine ganze Funktion 2. Grades einer Veränderlichen r, die die natürliche Zahlenreihe von $-\infty$ bis $+\infty$ durchwandert, Differenz θ soll das dem Minuenden entsprechende Quadrat der gesuchten Zerlegung werden. Die gegebene Zerlegung sei

$$M = ax_0^2 + cy_0^2,$$

die gesuchte

$$M = ax^2 + cy^2,$$

$ac = \Delta_1$. Dann ist:

(1) $ax_0^2 + cy_0^2 = ax^2 + cy^2$ und weiter (2) $ax_0^2 - c(y^2 - y_0^2) = ax^2$.

Erinnert man sich der auf S. 46 getroffenen Festsetzungen, so muß a prim zu c, y_0 u. y u. mithin in $y^2 - y_0^2 = (y + y_0)(y - y_0)$ enthalten sein. Ist a prim, so teilt a entweder $y + y_0$ oder $y - y_0$; ist es zusammengesetzt, so wird i. A. ein Faktor a' von a in $y + y_0$, der andere a'' in $y - y_0$ aufgehen. Eines der beiden Außenglieder a u. c muß notwendig ungerade sein. Da die Methode ihre Vertauschung zuläßt, kann man unbeschadet der Allgemeinheit a als ungerade annehmen. Weil ein gemeinsamer Teiler von a' u. a'' auch in $2y$ u. $2y_0$, mithin in

y u. y_0 aufgehn müßte, y u. y_0 aber zu a prim sind, müssen es auch a′ u. a″ untereinander sein. Man setzt an:

$$y + y_0 = a' \cdot p, \quad y - y_0 = a'' \cdot q;$$

dann

$$y^2 - y_0^2 = apq,$$

und (2) geht nach einer Division durch a zurück auf

$$(3) \quad x_0^2 - c \cdot p \cdot q = x^2.$$

Die beiden Unbestimmten p u. q gestatten aber ihre Ersetzung durch eine einzige r. Aus ihren beiden Definitionsgleichungen folgt nämlich:

$$(4) \quad 2y_0 = a'p - a''q.$$

Bestimmt man dann die Lösungen α′ u. α″ der unbestimmten Gleichung

$$(5) \quad a''\alpha' - a'\alpha'' = 1,$$

d. h. in der Eulerschen Ausdrucksweise den Bruch $\frac{\alpha'}{\alpha''}$, der dem andern $\frac{a'}{a''}$ am nächsten steht, oder in der Gaußschen Terminologie die mögliche Wurzel α′ der linearen Kongruenz $a''\alpha' \equiv 1 \pmod{a'}$, so läßt sich an der Hand von (4) substituieren:

$$(6_a) \quad p = a'' \cdot r - 2\alpha''y_0,$$

woraus für q hervorgeht:

$$(6_b) \quad q = a'r - 2\alpha'y_0.$$

Damit formt sich (3) um in

$$(7) \quad x_0^2 - c(a''r - 2\alpha''y_0)(a'r - 2\alpha'y_0) = x^2.$$

Führt man schließlich für den Subtrahenden von (7) die Abkürzung S ein, so entsteht für die Untersuchung die Forderungsgleichung

$$(8) \quad x_0^2 - S = x^2,$$

die jene, soviel Mal es angeht, erfüllen muß, wobei sie r alle möglichen ganzzahligen Werte beilegen kann. Geschieht dies auf- und abwärts von 0 in der natürlichen Ordnung, und wird die Ordnungszahl eines Gliedes aus der Reihe der S nach dem Werte seiner Veränderlichen gebildet, so ist die Differenz zwischen dem (r + 1).ten und r., anderseits zwischen dem — r. und — (r + 1). Gliede

$$= c[(2r + 1)a - 2y_0(a'\alpha'' + a''\alpha')],$$

bzw. $$- c[(2r + 1)a + 2y_0(a'\alpha'' + a''\alpha')].$$

Die Reihe der S gibt sich demnach als eine arithmetische Progression 2. Ordnung mit der konstanten Differenz

$2\Delta_1$ zu erkennen. Zwecks Vereinfachung des Subtraktionsprozesses spaltet man sie entsprechend positiven und negativen Werten der r in 2 Unterreihen I und II, die von dem 0. Gliede ausgehen. In beiden zieht man also von x_0^2 zunächst $4n\mu'\mu''y_0^2$, sodann von $x_0^2 - 4n\mu'\mu''y_0^2$ in I $c[1 \cdot a - 2y_0(a'\alpha'' + a''\alpha')]$, in II $c[1 \cdot a + 2y_0(a'\alpha'' + a''\alpha')]$, hierauf in beiden Reihen von der neuerstandenen Differenz einen um $2\Delta_1$ größeren Subtrahenden u. s. f. ab, bis schließlich θ von positiven zu negativen Werten übergeht. Wird schon $\theta = x_0^2 - 4n\mu'\mu''y_0^2 < 0$, so unterbleibt die Reihe ausnahmslos positiver S gänzlich. Das zu x gehörige y geht unter Benutzung des x entsprechenden r etwa aus der Gleichung $y + y_0 = a'p$ hervor, welche liefert:

$$y = ar - 2a'\alpha''y_0 - y_0,$$

oder weil $a''\alpha' - a'\alpha'' = 1$,

$$y = ar - y_0(a'\alpha'' + a''\alpha').$$

Da a′ und a″ mit jedem andern zueinander primen Faktorenpaar vertauschbar sind, in das sich a zerlegt, so muß die Methode an allen diesen wiederholt werden. Indem aber r und mithin auch y sich positive und negative Werte zueignen können, so läßt sich die durchgängige Teilbarkeit von $(y + y_0)$ oder $(y - y_0)$ durch einen beliebigen Primteiler von a annehmen. Bezeichnet danach $n + 1$ die Anzahl aller verschiedenen Primteiler von a, so gestatten n derselben eine

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$$

fache Zusammenfassung zu 2 relativ primen Faktoren. Da 7 unter den 65 Δ_1 4 verschiedene Primteiler enthalten, nämlich

$$\begin{aligned} 210 &= 2 \cdot 3 \cdot 5 \cdot 7, & 330 &= 2 \cdot 3 \cdot 5 \cdot 11, \\ 462 &= 2 \cdot 3 \cdot 7 \cdot 11, & 840 &= 2^3 \cdot 3 \cdot 5 \cdot 7, \\ 1320 &= 2^3 \cdot 3 \cdot 5 \cdot 11, & 1365 &= 3 \cdot 5 \cdot 7 \cdot 13, \\ & & 1848 &= 2^3 \cdot 3 \cdot 7 \cdot 11, \end{aligned}$$

so kann die Form (a, 0, c), $ac = \Delta_1$, eine 8fache Subtraktionsrechnung fordern. Ist a prim, so erledigt sich diese durch Entwicklung einer einzigen Subtraktionsdoppelreihe. Möglichst große Δ_1 begünstigen offenbar die Raschheit des Verfahrens; je mehr Δ_1 bei konstantem M wächst, desto geringer wird die Gliederzahl der Reihen S und θ.

Nach der dargelegten Methode prüft Euler Zahlen, die in die beiden kongruenten Formen $40x^2 + 13y^2$ und $1848x^2 + y^2$ eingehen, und stellt eine Reihe von 22 Primzahlen in der Form $1848x^2 + 197^2$ fest, die mit 55 441 für $x = 3$ anfängt und mit 18 518 809 für $x = 100$ schließt. An dieser Stelle sollen Zahlen M in kongruenten Formen mit $\Delta_1 = 408$ behandelt werden.

1) Zur Untersuchung diene die Form (17, 0, 24), in der also $a = 17$, $c = 24$ ist. Gl. (2) wird:

$$17x_0^2 - 24(y^2 - y_0^2) = 17x^2;$$

die Substitution vereinfacht sich hier zu: $y + y_0 = 17r$, $y = 17r - y_0$, $y - y_0 = 17r - 2y_0$, somit folgt als Gl. (7):

$$x_0^2 - 24r(17r - 2y_0) = x^2.$$

Da allgemein jede ganze Funktion n. Grades einer Veränderlichen für ganze Werte derselben eine arithmetische Reihe n. Ordnung darstellt, so folgen die Subtrahenden $S = 24r(17r - 2y_0)$ in einer arithmetischen Progression 2. Ordnung aufeinander, deren 0., 1. und —1. Glied bzw. die Werte 0, $24(17 - 2y_0)$, $24(17 + 2y_0)$ haben und deren konstante Differenz $2\Delta_1 = 816$ beträgt. Von x_0^2 gelangt also zunächst $24(17 \mp 2y_0)$, hierauf von $x_0^2 - 24(17 \mp 2y_0)$ ein um $2\Delta_1$ größerer Subtrahend u.s.f. zum Abzug.

α) $M = 553\,361 = 17 \cdot 19^2 + 24 \cdot 151^2$

$x_0 = 19$, $y_0 = 151$, $24(17 \mp 2y_0) = -6840$, bzw. $= +24 \cdot 319$. Da $361 < 24 \cdot 319$, fällt Reihe II gänzlich fort.

I.				
361	22 825	32 233	28 585	
+ 6 840	+ 3 576	+ 312	− 2 952	
7 201	26 401	32 545	25 633	
+ 6 024 r = 2, y = −117	+ 2 760	− 504 r = 10, y = 19	− 3 768	
13 225 = 115²	29 166	32 041 = 179²	21 865	
+ 5 208	+ 1 944	− 1 320	− 4 584	
18 433	31 105	30 721	17 281	
+ 4 392	+ 1 128	− 2 136	− 5 400 r = 16, y = 121	
22 825	32 233	28 585	11 881 = 109²	
			6 216	
			5 665	

Im ganzen finden 4 Zerlegungen von 553 361 in (17, 0, 24) statt, nämlich: $553\,361 = 17 \cdot 19^2 + 24 \cdot 151^2 = 17 \cdot 115^2 + 24 \cdot 117^2 = 17 \cdot 179^2 + 24 \cdot 19^2 = 17 \cdot 109^2 + 24 \cdot 121^2$.

Aus ihnen entwickelt man die Primfaktoren von M nach dem Verfahren von S. 22. $\frac{p_1}{q_1} = \frac{19 \pm 115}{151 \pm 117} = \frac{1}{2}$, $\frac{p_2}{q_2} = \frac{19 \pm 179}{151 \pm 19} = -\frac{16}{17}$; $\frac{p_3}{q_3} = \frac{19 \pm 109}{151 \pm 121} = -3$

$$\frac{p_1'}{q_1'} = \frac{ap_1^2}{cq_1^2} = \frac{17}{24 \cdot 2 \cdot 2} = \frac{17}{96},\ p_1' + q_1' = 113$$

$$\frac{p_2'}{q_2'} = \frac{ap_2^2}{cq_2^2} = \frac{17 \cdot 16 \cdot 16}{24 \cdot 17 \cdot 17} = \frac{32}{51},\ p_2' + q_2' = 83$$

$$\frac{p_3'}{q_3'} = \frac{ap_3^2}{cq_3^2} = \frac{17 \cdot 3 \cdot 3}{24} = \frac{51}{8},\ p_3' + q_3' = 59.$$

Es weist demnach 553 361 die Primteiler 59, 83 und 113 zu; in der Tat ist 553 361 gleich ihrem Produkte.

β) $M = 208\,001 = 17 \cdot 5^2 + 24 \cdot 93^2$

$x_0 = 5$, $y_0 = 93$, $24(17 \mp 2y_0) = -4056$, bzw. $= +24 \cdot 203$. Reihe II verschwindet wiederum.

I.						
25	7 321	11 353	12 121	9 625	7 153
+ 4 056	+ 2 424	+ 792	— 840	— 2 472	— 3 288
4 081	9 745	12 145	11 281	7 153	3 865
+ 3 240	+ 1 608	— 24	— 1 656		
7 321	11 353	12 121	9 625		

Da θ nirgends quadratisch wird, bekundet sich damit 208 001 als prim.

2. Man legt die Form (51, 0, 8) zugrunde; $a = 51$, $b = 8$. Gl. (2): $51x_0^2 - 8(y^2 - y_0^2) = 51x^2$.

$y^2 - y_0^2$ kann nun derart durch 51 geteilt werden, daß es entweder die Summe $y + y_0$ wird oder daß diese den Faktor 17, die Differenz $y - y_0$ den Faktor 3 enthält. In jenem Falle substituiert man a) $y + y_0 = 51r$, $y = 51r - y_0$, $y - y_0 = 51r - 2y_0$, mithin kommt als Gl. (7):

$x_0^2 - 8r(51r - 2y_0) = x^2$; in diesem b) $y + y_0 = 17p$, $y - y_0 = 3q$ ($a' = 17$, $a'' = 3$); der Gl. (5): $3\alpha' - 17\alpha'' = 1$ genügen die Werte $\alpha' = 1$ und $\alpha'' = 6$, damit ersetzt man weiter (6a): $p = 3r - 12y_0$, (6b): $q = 17r - 2y_0$, woraus (7) entsteht: $x_0^2 - 8(3r - 12y_0)(17r - 2y_0) = x^2$. Der Subtrahend S ist in (a) $S = 8r(51r - 2y_0)$, in (b) $S = 8(3r - 12y_0)(17r - 2y_0)$; in beiden Fällen bildet er eine arithmetische Progression 2. Ordnung mit der konstanten Differenz $2\Delta_1 = 816$. o., 1. und — 1. Glied sind in (a) bzw. o, $8(51 - 2y_0)$, $8(51 + 2y_0)$; in (b) bzw.

$192y_0^2$, $8(51 - 70y_0)$, $8(51 + 70y_0)$. Jede der beiden Substitutionen verlangt eine gesonderte Subtraktionsrechnung. Man gibt:

α) $M = 229\,067 = 51 \cdot 67^2 + 8 \cdot 4^2$

a) $x_0 = 67$, $y_0 = 4$; $8(51 \mp 2y_0) = 344$, bzw. $= 472$.

I.			II.		
	4 489	2 985		4 489	2 729
	− 344	−1 976		− 472	−2 104 r = −3
	4 145	1 009		4 017	y = − 157 625 = 25^3
	−1 160			−1 288	
	2 985			2 729	

b) $p = 3r - 48$, $q = 17r - 8$, $S = 8(3r - 48)(17r - 8)$; o., 1. und — 1. Glied der Reihe S bzw. $= 3072$, $3072 - 1832$, $3072 + 1832$; Reihe II erübrigt sich.

I.				
	4 489	3 249	4 465	2 417
	− 3 072	+1 016	− 616	−2 248 r = +6
	1 417	4 265	3 849	169 = 13^2
	+1 832 r = +1	+ 200	−1 432	
	3 249 = 57^2	4 465	2 417	

Zu der gegebenen Zerlegung von M in (51, 0, 8) treten also noch 3 andere, nämlich: $M = 51 \cdot 25^2 + 8 \cdot 161^2 = 51 \cdot 57^2 + 8 \cdot 89^2 = 51 \cdot 13^2 + 8 \cdot 266^2$. Die Primteiler von M liefern die Brüche

$$\frac{p_1}{q_1} = \frac{67 \pm 57}{4 \pm 89} = \frac{4}{3}, \quad \frac{p_2}{q_2} = \frac{67 \pm 13}{4 \pm 166} = \frac{8}{17}, \quad \frac{p_3}{q_3} = \frac{57 \pm 13}{89 \pm 166} = \frac{14}{51}.$$

$$\frac{p_1'}{q_1'} = \frac{ap_1^2}{cq_1^2} = \frac{51 \cdot 4^2}{8 \cdot 3^2} = \frac{34}{3}, \quad p_1' + q_1' = 37$$

$$\frac{p_2'}{q_2'} = \frac{ap_2^2}{cq_2^2} = \frac{51 \cdot 8^2}{8 \cdot 17^2} = \frac{24}{17}, \quad p_2' + q_2' = 41$$

$$\frac{p_3'}{q_3'} = \frac{ap_3^2}{cq_3^2} = \frac{51 \cdot 14^2}{8 \cdot 51^2} = \frac{49}{102}, \quad p_3' + q_3' = 151$$

229 067 setzt sich also aus den Primteilern 37, 41 und 151 zusammen.

β) $M = 541\,091 = 51 \cdot 103^2 + 8 \cdot 2^2$

a) $x_0 = 103$, $y_0 = 2$, $8(51 \mp 2y_0) = 376$, bzw. $= 440$.

I.			II.		
	10 609	7 033		10 609	6 841
	− 376	−2 824		− 440	−2 888
	10 233	4 209		10 169	3 953
	− 1 192	−3 640		− 1 256	−3 704
	9 041	569		8 913	249
	− 2 008			− 2 072	
	7 033			6 841	

b) $p = 3r - 24$, $q = 17r - 4 \cdot 0.$, 1. u. -1. Glied der Reihe S bzw. $= 768$, $768 - 712$, $768 + 1528$.

I.			II.	
10 609	9 529		10 609	5 969
− 768	− 1 736		− 768	− 3 160 r = − 3
9 841	7 793		9 841	2 809 = 53²
+ 712	− 2 552		− 1 528	
10 553	5 241		8 313	
− 104	− 3 368		− 2 344	
10 449	1 873		5 969	
− 920				

M zerlegt sich also auf doppelte Weise in (51, 0, 8): $M = 51 \cdot 103^2 + 8 \cdot 2^2 = 51 \cdot 53^2 + 8 \cdot 223^2$; daraus gehen die Primteiler 71 und 7621 von $M = 541\,091$ hervor.

γ) $M = 571\,811 = 51 \cdot 103^2 + 8 \cdot 62^2$.

$$x_0 = 103,\ y_0 = 62,\ y_0^2 = 3844.$$

a) $8\,(51 \mp 2y_0) = -584$, bzw. $= 1400$.

I.			II.	
10 609	9 913		10 609	3 961
+ 584	− 1 864		− 1 400	− 3 848
11 193	8 049		9 209	113
− 232	− 2 680		− 2 216	
10 961	5 369		6 993	
− 1 048	− 3 496		− 3 032	
9 913	1 873		3 961	

b) $p = 3r - 744$, $q = 17r - 124$.

0. und 1. Glied der Reihe S bzw. $= 738\,048$ und $738\,048 - 34\,312$. Reihe II ist untauglich und Reihe I solange, als die θ negativ bleiben. Man berechnet in I diejenigen Glieder, die den Wert 10 609 einschließen, und setzt von ihnen aus die Subtraktion fort. Setzt man nämlich das r. Glied von I: $738\,048 - 34\,312r + \frac{r\,(r-1)}{2}\,816 = 10\,609$, so wird die kleinere Wurzel dieser Gleichung von 2 ganzen Zahlen eingeschlossen, die die gesuchten Glieder der Reihe bestimmen. Die Gleichung zieht sich zusammen in $408 \cdot r^2 - 34\,720r + 727\,439 = 0$ und daraus angenähert $r^2 - 85r + 1783 = 0$, mithin

$$r = \frac{85}{2} \pm \sqrt{\left(\frac{85}{2}\right)^2 - 1783} \sim \frac{85}{2} \pm \sqrt{23} \sim \frac{85}{2} \pm 5.$$

Da θ von negativen zu positiven Werten übergehen muß, was das kleinere r bedingt, so muß zu dem negativem Vorzeichen gegriffen werden, und man hat:

$$37 < r < 38.$$

Das 37. Glied der Reihe I bewertet sich zu 11 960, das 38. zu 7840, ihre Differenz zu 4120.

I.			
10 609	6 073	11 089	8 761
— 11 960	+ 2 488	+ 40	— 2 408
— 1 351	8 561	11 129	6 353
+ 4 120	+ 1 672	— 776	— 3 224
2 769	10 233	10 353	3 129
+ 3 304	+ 856	— 1 592	
6 073	11 089	8 761	

Da θ in keiner der beiden Subtraktionsfolgen zum Quadrate wird, gehört 571 811 der Reihe der Primzahlen an.

Um Eulers Methoden ein Schlußwort hinzuzufügen, so eignen sie sich weit eher als ihre vorhergehenden zu praktischer Verwendung. Sie offenbaren den Reichtum und die Vielseitigkeit des Eulerschen Geistes, jedoch spiegeln sie das Verhältnis wieder, das ihr Verfasser zur Zahlentheorie eingenommen hat. Euler legte den Grundstein zum Gebäude jener Theorie, er brach sich als erster zu ihren wichtigsten Sätzen (Eulersches Kriterium, Reziprozitätsgesetz, Satz über die kongruenten Formen usw.) Bahn, allein nur eine induktive; den wenigsten hat er eine theoretische Begründung gegeben. Welche Mühe kostete ihn nicht der Nachweis des Fermatschen Satzes, daß jede Primzahl von der Form $4n + 1$ ein einziges Mal durch Addition 2er Quadrate entsteht! Seine Entdeckungen, so glanzvvoll und hervorragend sie auch waren, blieben Bruchstücke, die erst Gauß durch das Ferment des Determinantenbegriffes zu einer in sich abgeschlossenen Theorie verband. Dieser Mangel verschloß ihm die Mittel zur weitestgehenden Vereinfachung und Nutzbarmachung seiner Subtraktionsmethode, deren sich Gauß bedienen konnte. Ihr Wirkungskreis bleibt ein beschränkter. Wenn die Zahlen i. A. die erste Million übersteigen, so wird sie infolge ihrer Langsamkeit und Eintönigkeit aufgegeben werden und den Gaußschen Methoden weichen.

Die Gaußschen Methoden der Primzahlbestimmung.

Erst diese, welche in den Art. 329—334 der D. A. niedergelegt sind, können praktische Verwendung beanspruchen. Da bislang noch bessere ausstehen, haben sie noch nichts an ihrem Werte verloren, während den Eulerschen nur noch ein historischer zukommt. Indem ferner in sie hinein die gesamten

Ergebnisse der Theorie der quadratischen Reste und Formen verwoben sind, bieten sie sehr viel Abwechslung, ganz abgesehen davon, daß sie die Eulerschen an Kürze übertreffen. Im Eingangswort (Art. 329) verspricht Gauß von ihnen, daß sie vor allen andern bisher üblichen den Vorzug verdienen und daß er durch langjährige Erfahrung ihre Wirksamkeit erprobt hat, die selbst bei 8stelligen Zahlen noch anhält. Damit räumt er selbst als Grenze ihrer praktischen Brauchbarkeit etwa die Milliarde ein. Bevor man zu den Methoden selber greift, rät er die Division von M durch die niedrigsten Primteiler bis zu 19 mindestens an, einerseits damit nicht einige einfache Divisionen dasselbe leisten wie eine verwickelte längere Rechnung, andrerseits weil die aus den Divisionen entstandenen Reste später benützt werden. Er entwickelt 2 im Prinzip verschiedene Methoden. Die erste (Art. 330—332) baut sich auf der Theorie der quadratischen Reste; die zweite (Art. 333—334) auf derjenigen der quadratischen Formen auf.

1. Gaußsche Methode.

Ihre Grundlage.

Sie nimmt ihren Ausgangspunkt von dem Satze: Ist eine Zahl r quadratischer Rest einer andern M, so ist sie es auch von jedem Teiler von M. Denn gilt die Kongruenz:

$$x^2 \equiv r \pmod{M}$$

ist also die Differenz $x^2 - r$ durch M teilbar, so ist sie es auch durch jeden Faktor von M, womit der Satz unbeschränkt bewiesen ist.

Ihr Grundgedanke.

Von den Primzahlen, die M zusammensetzen, liegen alle bis vielleicht auf einen einzigen unterhalb $\sqrt{M}$. Bezeichnet man die Gesamtheit aller $\sqrt{M}$ voraufgehenden Primzahlen mit Ω, so sind in Ω auch die Primteiler von M, die $< \sqrt{M}$ sind, enthalten. Es bildet nun den Grundgedanken der Methode, den Komplex Ω durch Ausstoßung aller übrigen auf die Primteiler von M zurückzuführen. Es gelingt dies durch Anwendung des Eingangssatzes. Steht nämlich eine Zahl r als quadratischer Rest von M fest, so müssen offenbar aus Ω alle diejenigen Primzahlen ausgeschlossen werden, für welche r Nichtrest wird, wodurch die Gliederzahl in Ω ungefähr auf die Hälfte

herabgeht. Andere Reste r', r'', r''' .... wirken in derselben Weise wie r. Schließlich werden nur noch so wenige Glieder in Ω zurückbleiben, daß die Division von M durch diese der Arbeit einer weiteren Ausschließung gleichkommt. Sollen die Exkludenten ihren Zweck erfüllen, so müssen sie sämtlich voneinander unabhängig sein, d. h. das Produkt von beliebig vielen unter ihnen darf kein Quadrat bilden. Gilt nämlich $r \cdot r' \cdot r'' \cdot r''' \ldots . r^{(m)} = R^2$, und sind sämtliche Reste bis auf den letzten $r^{(m)}$ als Exkludenten benutzt worden, so enthält Ω nur noch solche Primzahlen, die mit M in jenen Resten und mithin auch in ihrem Produkte als Rest übereinstimmen. Wie aus dem Satze des Art. 98 hervorgeht, ist aber $r^{(m)}$ von allen diesen ebenfalls Rest und kann somit keine unter ihnen ausschließen. Ausgenommen sind nur die Primteiler, welche r, r', r'' .... $r^{(m-1)}$ zusammensetzen, welche einzig und allein als Nichtreste von $r^{(m)}$ ausgeschlossen werden können. Ein von andern abhängiger Rest kann also i. A. als Exkludent keine Verwendung finden.

Die beiden Kernpunkte der Methode.

Die Methode stellt also zweierlei Aufgaben: 1. quadratische Reste der zu untersuchenden Zahl M zu finden und 2. mit diesen die Ausschließungen im Primzahlkomplex Ω vorzunehmen. Da die Lösung der 2. Aufgabe zeigt, daß dieser nicht allgemein alle Reste, sondern nur diejenigen eines bestimmten Intervalles genügen, somit die Lösung der 1. Aufgabe von ihr abhängt, so muß ihre Behandlung vorangehen.

Die Primzahlen, die den quadratischen Rest r von M als Nichtrest haben, sind in einer Gruppe von linearen Formen $(4)r + n$ enthalten, deren Modul r oder 4r ist und deren linearer Rest n nach den Vorschriften der D. A. Art. 147—150 bestimmt wird. Mithin treten alle Primzahlen, die eine jener Formen annehmen, aus Ω heraus. Zur Ausführung der Ausschließung ist also die Kenntnis der Nichtteilformen von r erforderlich. Ist r klein, so entsprechen ihm nur wenige jener Formen: $r = -1 — 4n + 3$; $r = +2 — 8n + 3, 5$; $r = -2 — 8n + 5, 7$; $r = -3 — 3n + 2$ usw. Nun aber entziehen sich im allgemeinen Falle die Minimalreste der Feststellung. Allerdings zeigen einfache Divisionen, ob M in den Teiler- oder Nichtteilerformen der kleinsten Zahlen erscheint. Jedoch gehen daraus nur quadratische Nicht-

reste von M hervor. Denn der erste Fall lehrt, daß jene Nichtreste einer geraden Anzahl Primteiler von M, der zweite, daß sie auf jeden Fall Nichtreste von M sind, wodurch beidemale das Ausschließungsverfahren nicht gefördert wird. Benützt man zur Ausschließung die Nichtteilerformen eines größeren Restes r von M, so beeinträchtigt die wachsende Zahl derselben die Kürze der Rechnung. Im allgemeinen Falle muß man auf ihre Hilfe verzichten. Vielmehr wird man den Fortfall jeder Vorarbeit zur Ausschließung oder ein Hilfsmittel fordern, das die Ergebnisse von jener für alle Reste r, allerdings innerhalb eines begrenzten Gebietes, in sich schließt. Ein solches bietet aber eine Tafel dar, die jedem einzelnen jener r den quadratischen Charakter bezüglich aller p von Ω zuweist. Gauß empfiehlt dabei, die Einrichtung einer solchen Tafel nach dem Muster derjenigen vorzunehmen, die er den D. A. (vgl. Anh.) beigefügt hat. Danach wurde auch die Tafel I dieser Arbeit angelegt.

Einrichtung der Tafel I.[1])

Sie enthält in ihrer mittleren Vertikalspalte alle Primzahlen von 3 bis 997 als unverminderten Komplex Ω, in ihrer obersten Horizontalspalte die Restzahlen r_0 von $-100+100$ und zwar in der rechten Hälfte die von $+2$ bis $+100$, in der linken die von -1 bis -100. Da alle in δ und r_0 nicht aufgehenden Primzahlen mit dem Rest oder Nichtrest $\delta^2 r_0$ gleichzeitig den Rest oder Nichtrest r_0 besitzen, können aus der Reihe der r_0 alle Quadratzahlen selber und alle durch diese teilbaren Zahlen entfernt werden. Jedem r_0 entspricht also eine Vertikal-, jedem p eine Horizontalspalte, ihr Schnittquadrat nimmt die Bezeichnung des quadratischen Charakters von r_0 zu p auf. Je nachdem $r_0 R p$ oder $r_0 N p$, enthält es nach Gaußschem Vorbild entweder einen Horizontalstrich oder bleibt ganz frei. Die Vertikalspalte von r_0 übermittelt somit alle Primzahlen bis zu 1000, die im Reste oder Nichtreste r_0, die Horizontalspalte von p alle Zahlen r_0, die im Modul oder Nichtmodul p übereinstimmen. Hat man nach den im Folgenden auseinanderzusetzenden Methoden einige Reste r aus dem Bereiche der r_0 gewonnen, so faßt man unter Übergehung der andern die diesen r entsprechenden Vertikalspalten ins Auge und vergleicht sie daraufhin, ob sich irgend eine

[1]) Wurde bei der Drucklegung der Arbeit weggelassen.

Horizontalspalte durch eine lückenlose Aufeinanderfolge von Reststrichen auszeichnet. Entdeckt man eine solche, so ist meistens der zugehörige Modul p ein Primteiler von M. Im entgegengesetzten Falle erweist sich damit M als eine Primzahl.

Um die Übersicht über die Vertikalspalten der r zu erleichtern, schlägt Gauß vor, sämtliche Vertikalspalten herauszuschneiden und auf Holz- oder Blechstreifen aufzukleben, wodurch die Ausschließungstafel in einen Ausschließungsapparat übergeht, dessen sich zu bedienen Gauß sonst noch öfters anrät. Greift man dann aus der Sammlung aller Stäbchen diejenigen der r heraus und legt diese so nebeneinander, daß die Kopfzahlen r in eine Horizontalspalte fallen, so lassen sich die etwaigen Primfaktoren von M auf den ersten Blick erkennen. Hat man also einmal die Reste r festgestellt, so kann die Ausschließung durch Zuhülfenahme der Tafel oder des Apparates rein mechanisch, ohne jegliche frische Rechenarbeit bewerkstelligt werden. Der Ausschließungsapparat wirkt also gewissermaßen wie eine moderne Rechenmaschine.

Vieldeutigkeit der Gaußschen Methode.

Gauß entwickelt seine Ausschließungsmethode, ohne ihre Eindeutigkeit zu prüfen. Es entsteht nämlich die Frage, ob es nicht mehrere Primzahlen in Ω gibt, denen die gleichen Reste entsprechen, d. h. ob die Primteiler von M eindeutig oder mehrdeutig bestimmt sind.

Hat eine Primzahl p die Reste $r_1, r_2 \ldots r_n$, so kommt sie in den Teilerformen der r vor, d. h. es bestehen die Gleichungen:

$$(1)\ p = \alpha_1 r_1 c_1 + a_1 = \alpha_2 r_2 c_2 + a_2 = \alpha_3 r_3 c_3 + a_3 = \text{——} \ldots = \alpha_n r_n c_n + a_n,$$

in denen die Koeffizienten α je nach dem Reste von r bezüglich 4 entweder $= 1$ oder $= 4$ sind; oder die Kongruenzen

$$(1_a)\ p \equiv a_1 \pmod{\alpha_1 r_1} \equiv a_2 \pmod{\alpha_2 r_2} \equiv a_3 \pmod{\alpha_3 r_3} \ldots\ldots \equiv a_n \pmod{\alpha_n r_n}.$$

Bezeichnet man nun mit p_0 den positiv kleinsten Rest der Restklasse, der p in bezug auf den Modul $\overline{\lfloor \alpha r \rfloor}$ angehört, so besteht die Kongruenz: $p \equiv p_0 \pmod{\overline{\lfloor \alpha r \rfloor}}$ oder die Gleichung

$p = p_0 + c \cdot \overbrace{\lceil \alpha r \rfloor}$. Ihre rechte Seite stellt für laufendes c eine arithmetische Reihe 1. Ordnung mit dem Anfangsglied p_0 und der Differenz $\overbrace{\lceil \alpha r \rfloor}$ dar. Da beide zueinander prim sind, enthält sie nach dem Satze über die arithmetische Progression unendlich viele Primzahlen p, die sämtlich den Gleichungen (1) und Kongruenzen (1_a) genügen, d. h. dieselben Reste $r_1, r_2, r_3 \ldots\ldots r_n$ gemein haben. Das Intervall $0 — \overbrace{\lceil \alpha r \rfloor}$ kann also von der Menge der p höchstens eines, nämlich p_0, falls p_0 prim ist, enthalten. Wurde oben eine Primzahl als gemeinschaftlicher Modul beliebig vieler Reste vorausgesetzt, so legt man nunmehr die Frage vor, ob allgemein beliebig viele Zahlen r quadratische Reste einer und derselben Primzahl x werden können.

Gegeben sei die Zahlenmenge $r_1, r_2, r_3 \ldots\ldots r_n$; gesucht alle Primzahlen x, die in den auf sie bezogenen quadratischen Charakteren der r oder in den Werten der Legendreschen Symbole $\left(\frac{r}{x}\right)$ übereinstimmen (und die nicht in den r aufgehen).

Reduktionen der r.

1. Da jede Primzahl x neben einem Reste $r\,\delta^2$ auch diesen r besitzt, so können sämtliche r von ihren quadratischen Faktoren befreit werden.

2. Eine zweite Vereinfachung der r erfolgt nach dem Satze der D. A. Art. 98: Das Produkt zweier Reste oder Nichtreste einer Primzahl x gibt einen Rest, dagegen dasjenige eines Restes und Nichtrestes einen Nichtrest von x. Schließlich können sämtliche r als voneinander unabhängig angesehen werden, d. h. der quadratische Charakter keines von ihnen folgt aus dem der übrigen.

Charakterbedingungen.

$R_1, R_2, R_3 \ldots\ldots R_m$ geben die Reihe der reduzierten r an; man zerlege sie in ihre Primteiler:

$$\begin{aligned}
R_1 &= p_{11} \cdot p_{12} \cdot p_{13} \cdot \ldots\ldots p_{1m} \\
R_2 &= p_{21} \cdot p_{22} \cdot p_{23} \cdot \ldots\ldots p_{2m} \\
R_3 &= p_{31} \cdot p_{32}\ p_{33} \cdot \ldots\ldots p_{3m} \\
&\vdots \qquad\quad \vdots \qquad\qquad \vdots \\
R_m &= p_{m1}\, p_{m2}\, p_{m3} \cdot \ldots\ldots p_{mm},
\end{aligned}$$

unter welchen sich mit Einrechnung von — 1 1 verschiedene vorfinden mögen. Auf jedes R entfällt ein bestimmter quadratischer Charakter, auf seine Primteiler dagegen irgend eine in jenem

resultierende Charakterkombination. Die Charaktere der l verschiedenen p sind demnach m Bedingungen unterworfen.

Zahl der Charakterkombinationen, die diese Bedingungen wahren.

Sieht man zunächst von ihnen ab, so stehen jedem p 2 Charaktere — Rest und Nichtrest — offen, mithin bieten sich an den l Primteilern 2^m Charakterkombinationen dar. Unter Berücksichtigung der m unabhängigen Charakterbedingungen erhellt aber zunächst, daß jedes R einen Primteiler p enthalten muß, der sich in keinem andern R mehr findet. Daraus folgt, daß die Charaktere von l−m Primteilern p beliebig angenommen werden dürfen, daß dadurch aber diejenigen der m übrigen festgelegt sind. Da nun jenes auf 2^{l-m}fache Art erfolgen kann, so ergibt sich, daß 2^{l-m} Charakterkombinationen möglich sind, die sich den m Charakterbedingungen der R unterwerfen.

Die Linearformen von x.

x muß entweder in eine Teiler- oder in eine Nichtteilerform jeder der l Primzahlen p eingehen oder die l Kongruenzen befriedigen:

$$(2)\quad x \equiv a_1 \pmod{\alpha_1 p_1} \equiv a_2 \pmod{\alpha_2 p_2}$$
$$\equiv a_3 \pmod{\alpha_3 p_3} \ldots \equiv a_l \bmod \alpha_l p_l),$$

in denen die Koeffizienten α entweder = 1, 4 oder 8 sind, je nachdem p von der Form 4n + 1, 4n + 3 oder = 2 ist. Die Entscheidung über die Existenz der Primzahlen x hängt also davon ab, ob das lineare Kongruenzensystem (2) eine gemeinsame Wurzel besitzt oder nicht. Wir gliedern nach den 3 eben hervorgehobenen Fällen. a) Alle p sind ungerade und haben teils die Form 4n + 1, teils in gerader Anzahl die Form 4n + 3; jene werden durch p′, diese durch p″ gekennzeichnet; zu den p″ zähle auch −1. (2) kommt dann in die Form:

$$(2')\quad x' \equiv a_1' \pmod{p_1'} \equiv a_2' \pmod{p_2'} \equiv \ldots\ldots$$
$$\equiv a_1'' \pmod{p_1''} \equiv a_2'' \pmod{p_2''} \equiv \ldots\ldots$$

Da die Moduln von (2′) stets prim zueinander sind, hat (2′) stets eine gemeinsame Wurzel x′. Umfassen die p noch die gerade Primzahl 2, so ändert die Zusatzkongruenz: $x' \equiv 1, 3, 5, 7 \pmod 8$ nichts an dem vorhergehenden Ergebnis. b) Alle p sind ungerade und haben teils die Form 4n + 1, teils in ungerader Zahl die Form 4n + 3. Das Kongruenzensystem (2) formt sich dann um in

$$(2''): x'' \equiv a_1' \pmod{p_1'} \equiv a_2' \pmod{p_2'} \equiv \ldots$$
$$\equiv a_1'' \pmod{4p_1''} \equiv a_2'' \pmod{4p_2''} \equiv \ldots\ldots$$

Nunmehr sind nicht mehr sämtliche Moduln zueinander prim, sondern diejenigen, welche den p″ entsprechen, haben den Faktor 4 gemeinschaftlich. Um die Bedingung der gemeinsamen Lösung von (2″) zu erkennen, untersucht man daraufhin das Kongruenzensystem:

$$(3)\quad x \equiv b_1 \pmod{\delta z_1} \equiv b_2 \pmod{\delta z_2}$$
$$\equiv b_3 \pmod{\delta z_3} \equiv \ldots\ldots \equiv b_n \pmod{\delta z_n},$$

in dem alle Moduln den gemeinschaftlichen Teiler δ besitzen, die z aber zueinander prim sein sollen. Ersetzt man (3) durch (3′):

$$x' \equiv b_1 \pmod{z_1} \equiv b_2 \pmod{z_2} \equiv b_3 \pmod{z_3}$$
$$\equiv \ldots\ldots \equiv b_n \pmod{z_n} \equiv b_1 \pmod{\delta},$$

so kommt (3′), da alle seine Moduln relativ prim sind, eine gemeinschaftliche Wurzel x′ zu. Sind jetzt sämtliche b (mod. δ) einander kongruent, so ist nicht nur $x' - b_1$ teilbar durch δz_1, sondern allgemein $x' - b_i$ durch δz_i, d. h. x′ stellt auch (mod. $\delta z_1 z_2 \ldots z_n$) die gemeinsame Wurzel von 3 dar. Damit (2″) auflösbar werde, ist also die notwendige und hinreichende Bedingung, daß sämtliche a″ [mod. 4] kongruent sind. c) Die Primzahlen p in der Zusammenstellung von (b) enthalten zudem $p = 2$. Die Auflösbarkeit von (2″) scheitert in diesem Falle daran, daß die Moduln nach Entfernung ihres gemeinsamen Teilers noch nicht prim zueinander werden und somit die Analogie zu (3′) verloren geht. Deshalb muß (2″) dem Kongruenzensystem (2‴) weichen, dem die nach dem Modul $8p''$ genommenen Teiler- und Nichtteilerformen zugrunde gelegt sind.

$$(2'''): x''' \equiv a_1' \pmod{p_1'} \equiv a_2' \pmod{p_2'} \equiv \ldots\ldots$$
$$\equiv a_1''' \pmod{8p_1''} \equiv a_2''' \pmod{8p_2''} \equiv \ldots\ldots$$
$$\equiv a \pmod{8}.$$

Die gemeinsame Wurzel x‴ von (2‴) erfordert also nur, daß sämtliche $a''' \equiv a \pmod{8}$ sind.

In allen 3 Fällen tritt also eine gemeinsame Wurzel des Kongruenzensystemes (2) für eine beliebige Kombination linearer Reste a auf, oder x nimmt die Form an:

$$x = x_0 + c.\ 2^{\kappa} \overline{\lfloor p \rfloor}\quad \kappa \leq 2,$$

in der unzählig viele Primzahlen einbegriffen sind.

Zahl z der Restklassen des Moduls $2^3 \cdot \overline{\lfloor P \rfloor}$, in die sich die x verteilen.

Offenbar wird (2) soviele (mod. $2^\kappa \overline{\lfloor p \rfloor}$) inkongruente Lösungen gestatten, als die a Kombinationen eingehen können. Um die Anzahl derselben in eine für alle Fälle der Zusammensetzung der R gültige Formel zu fassen, werden durchlaufend die Teiler- und Nichtteilerformen von p auf den Modul 8p gebracht; jene seien durch $8p + r$, diese durch $8p + n$ ausgedrückt. Unter den l Primfaktoren, welche die Reihe der R zusammensetzen, seien L ungerade positive enthalten, wo also L entweder mit l zusammenfallen oder um 1 oder 2 von l abstehen wird. Sie seien mit P, ein beliebiger unter ihnen mit P_i bezeichnet. Gleichgültig welche Form P_i hat, so werden sich die Werte r_i und n_i gleichmäßig auf die 4 Formen $8n + 1, 3, 5, 7$ verteilen, sodaß auf jede derselben $\frac{P_i - 1}{2}$ Werte r_i und ebensoviele n_i entfallen.

Stehen P_i beide Charaktere offen, so kann in das Kongruenzensystem (II) der P jede Teiler- und Nichtteilerform von P_i eingeführt werden. Soll jedoch (II) eine gemeinsame Wurzel erlangen, so müssen sämtliche linearen Reste A von (II) einander (mod. 8) kongruent sein. Ein A_i kann sich also nur mit (mod. 8) gleichformigen A kombinieren, seine Stelle kann es, sich selbst noch einmal eingerechnet, mit $(P_i - 1)$ anderen tauschen.

Ist dagegen für P_i ein Charakter ausbedungen, so können die A_i in der festen Form $8n + \alpha$ nur den r_i oder n_i entnommen sein. Ihre Zahl beläuft sich demnach nur auf die Hälfte der vorigen, auf $\frac{P_i - 1}{2}$.

Sind M solcher Primteiler vorhanden, wo M und m ebenso zueinanderstehen wie L zu l, so folgt, daß sich die A von (II), die in der Form $8n + \alpha$ übereinstimmen,

$$2^{-M} (P_1 - 1) (P_2 - 1) \ldots (P_{l'} - 1)$$

mal, mithin sämtliche A von (II)

$$2^{-(M-2)} (P_1 - 1) (P_2 - 1) (P_3 - 1) \ldots (P_{l'} - 1)$$

mal kombinieren lassen. Die L Primzahlen P fallen entweder mit den p zusammen oder werden durch -1 und $+2$ zu ihnen ergänzt. Da (II) eine bestimmte Form $8n + \alpha$ von x vorschreibt, so können die beiden Zusatzkongruenzen: $x \equiv a_1$

(mod. 4) und $x \equiv a$ (mod. 8), welche (II) zu (2) vervollständigen, keine Vermehrung der Wurzelzahl von (II) erzeugen. Wird im Gegenteil von einem jener Werte oder von beiden ein Charakter gefordert, so sinkt z auf die Hälfte der Wurzelzahl von (II), bezw. ihren vierten Teil herab. Da aber dann die Menge m der Charakterbedingungen $= M + 1$, bezw. $= M + 2$ ist, da ferner jedes x prim zum Modul sein muß, erkennt man nachstehenden Satz:

Alle Primzahlen x, bezüglich derer n beliebige ganze Zahlen, die sich außer vielleicht in -1 und $+2$ in die l Primteiler $p_1, p_2, p_3 \ldots p_l$ zerlegen, n quadratische Charaktere einnehmen, die auf m unabhängige zurückgehen, ordnen sich in

$$z = 2^{-(m-2)} (p_1 - 1)(p_2 - 1) \ldots (p_l - 1)$$

relativ prime Restklassen des Moduls $2^3 \cdot p_1 \cdot p_2 \ldots p_l = 2^3 \overline{\lfloor p \rfloor}$ ein. Jede derselben umfaßt unzählig viele x.

Da irgend 2 $\left(\text{mod. } 2^3 \overline{\lfloor p \rfloor}\right)$ inkongruente Wurzeln x nach allen Faktormoduln mit Ausnahme eines einzigen kongruent sein können, nach diesem aber inkongruent sein müssen, so fallen, je nachdem eine gerade oder ungerade Anzahl unter den p, zu welchen auch -1 gezählt werde, von der Form $4n + 3$ ist, je 4 der Restklassen nach dem Modul $\overline{\lfloor p \rfloor}$ oder je 2 nach dem Modul $2^2 \overline{\lfloor p \rfloor}$ in eine zusammen. Im ersten Falle geht also ihre Zahl $\left(\text{mod. } \overline{\lfloor p \rfloor}\right)$ auf:

$$z' = 2^{-m} (p_1 - 1)(p_2 - 1) \ldots (p_l - 1),$$

im zweiten Falle $\left(\text{mod. } 2^2 \overline{\lfloor p \rfloor}\right)$ auf:

$$z'' = 2^{-(m-1)} (p_1 - 1)\, p_2 - 1) \ldots\ldots (p_l - 1)$$

zurück.

Um die Formel für z auf ihre Richtigkeit zu prüfen, vergleiche man sie zunächst mit der in den D. A. am Schluß des Art. 148 gegebenen, indem man sie auf eine zusammengesetzte Zahl C von der Form $4n + 1$ mit bestimmtem quadratischem Charakter anwendet. Da sämtliche Primteiler $p_1, p_2 \ldots p_l$ von C ungerade und eine gerade Menge unter ihnen von der Form $4n + 3$ sind, so verteilen sich alle Primzahlen x, die in dem festgesetzten Wert des Legendreschen Symbols $\left(\frac{C}{x}\right)$ übereinstimmen, auf

$$z' = \frac{1}{2}(p_1 - 1)(p_2 - 1) \ldots . (p_l - 1)$$

Teiler-, bezw. Nichtteilerformen von C, welche überhaupt ihre Klasse erschöpfen müssen, ein Ergebnis, das durch die angeführte Stelle bestätigt wird.

In zweiter Linie möge ein praktisches Beispiel die Formel für z erproben. Gesucht werden alle Primzahlen x, die in den Resten — 1, 5, 13, 17 übereinstimmen. Hier ist $l = m = 4$. 3 der l haben die Form $4n + 1$, ein einziges, nämlich — 1, die Form $4n + 3$. Nach der zweiten Spezialformel von oben gehören die x

$$z'' = 2^{-3}(5 - 1)(13 - 1)(17 - 1) = 96$$

relativ primen Restklassen des Moduls $2^2 \cdot 5 \cdot 13 \cdot 17 = 4420$ an. Überzeugt man sich induktiv von dieser Anzahl, so werden die x den Kongruenzen genügen:

$$(4)\quad x \equiv a_{(-1)} \pmod 4 \equiv a_{(5)} \pmod 5$$
$$\equiv a_{(13)} \pmod{13} \equiv a_{(17)} \pmod{17},$$

in denen den verschiedenen a die Werte freistehen: $a_{(-1)} \equiv 1 \pmod 4$ $a_{(5)} \equiv 1, 4 \pmod 5$; $a_{(13)} \equiv 1, 3, 4, -1, -3, -4 \pmod{13}$; $a_{17} \equiv 1, 2, 4, 8, -1, -2, -4, -8 \pmod{17}$. Da die a im ganzen 96 Kombinationen gestatten und jeder derselben eine Wurzel x von (4) entspricht, so erhellt in der Tat die Verteilung der x in 96 Restklassen des Modulus $4 \cdot 5 \cdot 13 \cdot 17 = 4420$ oder auf 96 Formen

$$4420 \cdot c + x_0,$$

in denen die x_0 die kleinsten positiven Auflösungen des Kongruenzensystemes (4) bezeichnen.

Der einfachste Weg zu ihrer Ermittlung führt über die entsprechende für die 3 letzten Kongruenzen:

$$(4')\quad x \equiv a_{(5)} \pmod 5 \equiv a_{(13)} \pmod{13} \equiv a_{(17)} \pmod{17}.$$

Da $a_{(5)}$, $a_{(13)}$ und $a_{(17)}$ sich in Paare entgegengesetzter Werte zerlegen, trifft solches auch für die 96 (mod. 1105) inkongruenten Wurzeln von (4') zu. Deshalb genügt die Berechnung von 48 Lösungen x' von (4'). Unterwirft man diese und ihre entgegengesetzten Werte noch der Bedingung $\pm x' \equiv 1 \pmod 4$, so gelangt man in den Besitz der 96 linearen Reste x_0. Die erste Zusammenstellung I gibt die 48 entgegengesetzten, absolut kleinsten Wurzelpaare von (4'), die zweite II die 96 x_0 wieder.

I.

± 1, 4, 9, 16, 49, 64, 66, 69, 81, 94, 101, 121, 134, 144, 166, 179, 186, 190, 196, 251, 256, 259, 264, 274, 276, 286, 321, 324, 339, 341, 361, 376, 389, 404, 406, 426, 441, 446, 451, 484, 491, 506, 511, 519, 529, 536.

II.

1, 9, 49, 69, 81, 101, 121, 321, 341, 361, 389, 441, 481, 529, 569, 621, 701, 729, 781, 829, 841, 849, 909, 961, 1041, 1069, 1089, 1101, 1109, 1121, 1141, 1169, 1249, 1301, 1361, 1369, 1381, 1429, 1481, 1509, 1589, 1641, 1681, 1769, 1821, 1849, 1869, 1889, 2089, 2109, 2129, 2141, 2161, 2201, 2209, 2389, 2401, 2461, 2469, 2549, 2609, 2661, 2701, 2721, 2729, 2809, 2869, 2889, 2909, 3041, 3129, 3181, 3221, 3249, 3381, 3409, 3449, 3481, 3501, 3589, 3601, 3721, 3741, 3821, 3901, 3909, 3921, 3929, 3969, 4021, 4029, 4081, 4161, 4169, 4229, 4241.

Da die Primzahlen x auch im Reste $-1 \cdot 5 \cdot 13 \cdot 15 = -1105$ übereinstimmen müssen, und da die Teiler- und Nichtteilerformen von — 1105 den Modul 4420 haben, so fallen offenbar die 96 Linearformen von x mit ebenso vielen Teilerformen von — 1105 zusammen.

Welchen Teil derselben bilden sie? Die Teilerformen $4420 \cdot c + r$ von — 1150 umfassen alle linearen Formen des Moduls 4420, in denen r 1. von der Form $4n + 1$ und Nichtrest von α) keinem oder β) zweien der Primfaktoren 5, 7, 13 2. von der Form $4n + 3$ und Nichtrest α) von einem oder β) von allen dreien ist. Nach den in den D. A. Art. 148 abgeleiteten Formeln umfassen die Gruppen 1α, 1β, 2α und 2β, bezw. 96, $96\left(\frac{3}{2}\right)$, $96\left(\frac{3}{1}\right)$ und $96\left(\frac{3}{3}\right)$ Werte r. Die 96 Formen $4420c + x_0$ machen somit nur den 8. Teil sämtlicher Teilerformen von — 1105 aus. Jedoch zeichnen sie sich vor allen andern dadurch aus, daß jede Primzahl, die sie annimmt, nicht nur als Rest — 1105, sondern jeden Primteiler von — 1105 hat. Nimmt man nun an, daß die Kenntnis der Reste — 1, 5, 13, 17 der untersuchten Zahl M sichersteht, und beschränkt man den Bereich Ω (vgl. S. 63) auf denjenigen der Tabelle I (vgl. S. 65), so entfallen auf diesen von den 96 x_0 die 23 ersten von 1 bis 961. Unter ihnen finden sich ohne Einrechnung der Einheit 5 Primzahlen x, nämlich 101, 389,

569, 701 und 829, welche, wie dies auch die Tabelle I zeigt, in den obigen Resten übereinstimmen müssen. Hätte man sich also in der Ermittlung der r (vgl. S. 63) mit diesen 4: — 1, 5, 13, 17 begnügt, so wäre aus dem Ausschließungsverfahren eine fünfdeutige Lösung hervorgegangen (vorausgesetzt, daß M, wie es wohl meistens zutreffen wird, nur aus 2 Primteilern besteht). Hebt man überhaupt die Ausschließungsmethode über ihre Einschränkung hinaus — ihr Urheber will sie im Vorwort zu seinen Methoden höchstens auf 8—9 stellige Zahlen angewendet wissen — gewährt man ihr unter Erweiterung des untersuchten Zahlenkreises einen immer größeren Spielraum, so nähert sie sich immer mehr dem Endzustand, daß ihre Ergebnisse ∞ vieldeutig werden. Hält man jedoch den Bereich Ω in engen Schranken, so wird schon für wenige kleinwertige r der Modul, in dessen Restklassen die x sich einfügen, die obere Grenze von Ω meist übertreffen, sodaß Ω von jenen höchstens ein x enthalten kann und sich mithin die Menge der x in Ω nach der Gesamtzahl z der Lösungen des Kongruenzensystems (2) bemißt (vgl. S. 68). Das behandelte Beispiel legte dar, daß schon die 4 kleinzahligen Reste — 1, 5, 13, 17 einen Modul bedingen, der über das vierfache Intervall Ω hinausragt, daß ferner von den 96 Lösungen des Kongruenzensystems (4) etwas weniger als der 4. Teil in Ω hineinfällt und von diesem wieder etwas mehr als der 4. Teil Primzahlen ergab, sodaß sich schließlich von den 96 möglichen Primzahlen x nur 5, d. h. noch nicht ihr 16. Teil verwirklichten. Immerhin zeugt es davon, daß selbst ein kleines Intervall keine Eindeutigkeit verbürgt. Jedoch wird eine geringe Vieldeutigkeit durch bloße Divisionen mühelos hinweggeräumt werden können. Hat somit die 2. Frage nach der Art der Ausschließung ihre Erledigung gefunden, so handelt es sich noch um die Genügeleistung der ersten.

4 Wege zur Ermittlung tauglicher Reste r.

Da die Verwendbarkeit der Reste r an den Bereich der Kopfzahlen r_0 der Tafel I gebunden ist, so können sich nur solche Reste eignen, 1) die selber, oder 2) deren Faktoren jenem Bereiche angehören. Gauß hat zu ihrer Ermittlung 3 hinreichend wirksame Methoden entwickelt, denen noch eine vierte an die Seite gestellt werden kann. Er schickt ihnen 2 Vorbemerkungen voraus.

α) Enthält der Rest r ein Quadrat und ist dieses prim zu M, was in der Regel für die untersuchten Zahlen M zutrifft, hat also die Zerlegung statt: $r = r' \cdot \rho^2$, so ist auch r' ein quadratischer Rest von M. Aus diesem Grunde werden sich Reste r mit großen Quadratzahlen als Faktoren oft gerade so gut eignen wie kleine r.

β) Zerlegt man jedes r in seine Faktoren und kombiniert dann diese, d. h. bildet man ihre Produkte, so werden diese unter allen Umständen wieder Reste von M darstellen. Treten dabei mehrere Faktoren in gerader Potenz auf, so können diese unter obiger Bedingung entfernt werden, wodurch es sich ereignen mag, daß aus dem gebildeten Produkte ein brauchbarer Rest hervorgeht. Die Kombination der Reste erweist sich also als ein wichtiges Hülfsmittel zu ihrer Vereinfachung.

In seinen 3 Methoden setzt Gauß den ganzen Apparat seiner arithmetischen Entdeckungen in Bewegung.

1. Methode.

Sie ist die einfachste und stützt sich auf keine weitere Theorie. Ihre Darstellung wird ihre Kennzeichnung als Summationsmethode rechtfertigen. Sie besteht darin, daß M oder ein Vielfaches von M zur Summe oder Differenz zweier Zahlen gemacht wird, deren negatives Produkt dann einen Rest von M gibt. Denn aus

$$k \cdot M = a + c$$

folgt:

$$ak \cdot M = a^2 + ac, \text{ mithin } a^2 \equiv -ac \pmod{M}, \quad \underline{-acRM.}$$

Damit der Rest $-ac$ sich eignet, müssen die Summanden a und c so gewählt sein, daß ihr Produkt durch ein großes Quadrat teilbar und der Quotient entweder eine kleine oder in solche zerlegbare Zahl wird. Es ist also von vornherein angezeigt, a als Quadrat oder als das Vielfache eines solchen anzunehmen, das von $k \cdot M$ nur um eine kleine oder in kleine Faktoren zerfällbare Zahl c absteht. Unter Anlehnung an die Theorie der quadratischen Formen wird man sich kurz so ausdrücken, daß man Darstellungen von $k \cdot M$ durch Formen mit verschwindendem Mittelgliede und kleinsten Außengliedern, also durch solche von der Gestalt (a, o, c) sucht, deren Determinante $-ac$ dann Rest von $k \cdot M$ und damit auch Rest von M sein wird. Unter der Annahme $k = 1$ geht man am zweckmäßigsten

dermaßen vor, daß man zunächst das einfache, hierauf das zweifache, dreifache, ... schließlich das nfache Quadrat bestimmt, das M am nächsten kommt, des weiteren die positive oder negative Differenz $M - ma^2$ nimmt und daraus ein geeignetes r abzuleiten trachtet. Als ein weiterer Algorithmus läßt sich der benützen, daß man ungefähr die 20 ersten Vielfachen von M, von $1 \cdot M$ bis $20 \cdot M$ bildet und dann der Tafel der Reihe nach die beiden Quadrate entnimmt, die jedes dieser Vielfachen einschließen. Fallen jene dabei aus dem Bereiche der Tafel heraus, so lassen sie sich durch Abstreichen der 2 oder erforderlicherweise 4 letzten Stellen jenem wieder zuführen. Auf diese Weise gewinnt man je 20 positive und negative Reste, von denen in der Regel die Hälfte sich als tauglich erweist.

Hülfssatz der 2. und 3. Methode.

Diese gehen auf folgenden Satz zurück: Gehören beliebig viele Formen demselben Geschlechte der Determinante D an, so sind alle aus einer geraden Anzahl ihrer Außenglieder gebildeten Produkte Reste von D. Den Beweis dieses Satzes stützt Gauß auf den Begriff der charakteristischen Zahl. Unter einer charakteristischen Zahl einer Form (a, b, c) versteht Gauß eine Zahl m, die den Kongruenzen genügt:

$$g^2 \equiv am,\ gh \equiv b \cdot m,\ h^2 \equiv cm \pmod{D}$$

er nennt dann das Symbol m(a, b, c) quadratischen Rest von D. In Art. 233 V der D. A. beweist er, daß, wenn eine zu D prime Zahl m sämtliche Spezialcharaktere der Form mit Ausnahme derjenigen bzgl. 4 und 8, wofern diese nicht in D aufgehen, angibt, m eine charakteristische Zahl der Form ist, woraus sich ihre Bezeichnung erklärt. Auf jeden Fall sind also, einerlei welche Potenz der 2 D teilt, alle durch (a, b, c) darstellbaren, zu D primen Zahlen charakteristische Zahlen von (a, b, c). Jedoch ist offensichtlich, daß diese nur einen Teil aller vorhandenen ausmachen, nämlich denjenigen, dem der Rest D zukommt. Zugleich erhellt, daß alle Formen des gleichen Geschlechts von D in ihren charakteristischen Zahlen übereinstimmen. So haben sämtliche Formen des Hauptgeschlechtes von D die charakteristische Zahl 1. Entfallen also die Formen

$$(a, b, c),\ (a', b', c'),\ (a'', b'', c'') \ldots\ldots$$

auf dasselbe Geschlecht von D und bedeutet m eine charakteristische Zahl desselben, so sind die Produkte

$$ma,\ mc,\ ma',\ mc',\ ma'',\ mc'' \ldots\ldots$$

sämtlich Reste von D. Bildet man dann alle möglichen Produkte aus je zweien, allgemein aus einer geraden Zahl derselben und streift den gemeinsamen Teiler m^2, bzw. m^{2n}, ab, da er prim zu D ist, so sind

$$ac,\ a'c',\ a''c'',\ ac',\ ac'',\ a'c,\ a''c \ldots\ldots$$
$$aca'c',\ aca''c'',\ a'c'a''c'',\ \ldots\ldots \qquad \ldots\ldots$$

ebenfalls lauter Reste von D, w. z. b. w.

Formen, welche also 1. ein positives oder negatives Vielfache der zu untersuchenden Zahl zur Determinante haben,

$$D = \pm k \cdot M \quad (k > 0)$$

und 2. demselben Geschlechte von D angehören, vereinigen eine gerade Menge ihrer Außenglieder als Faktoren zu Resten von $\pm k \cdot M$ und damit auch von M.

Wie findet man nun solche Formen?

Sie fließen aus 2 verschiedenen Quellen, nämlich 1. aus der Periode einer Klasse der positiven Determinante $+ k \cdot M$ und 2. aus einer solchen der negativen Determinante $- k \cdot M$.

2. Methode.

Sie schöpft aus der ersten Quelle. Wird nämlich nach dem Algorithmus des 2. Absatzes des Art. 186 die erstgenannte Periode gewonnen:

$$(A,\ B,\ -A'),\ (-A',\ B',\ A''),\ (A'',\ B'',\ -A'''),\ (-A''',\ B''',\ A'''')$$
$$\ldots\ldots\ldots\ (-A^{(m)},\ B^{(m)},\ A),$$

so gehören diese Formen, in denen die Werte A das gleiche, die Mittelglieder B das positive Vorzeichen besitzen, derselben Klasse und damit auch demselben Geschlechte von $D = k \cdot M$ an. Somit übermitteln die aus einer geraden Zahl ihrer Außenglieder zusammengesetzten Produkte

$$-AA',\ AA'',\ -AC',\ AC'',\ -A'A'',\ -C'A'' \ldots\ldots\ldots$$
$$AA'A'''A''',\ AA'C''C''',\ -A'C'A''A''',\ \ldots\ldots$$

Reste von $+ k \cdot M$ und folglich auch Reste von M.

Von großem Vorteil ist es, die Periode der Hauptklasse der Determinante $+ k \cdot M$ von der Hauptform $(1,\ 0,\ -k \cdot M)$

aus zu berechnen. Da in dieser $A = 1$ ist, so stellen schon die Außenglieder in der Periode selber Reste von M dar. Überhaupt erleichtern solche Ausgangsformen, in denen das Vorderglied A möglichst klein ist, die Bestimmung geeigneter r.

3. Methode.

Setzt man eine Klasse K der Determinante D mit ihren aufeinanderfolgenden Potenzen zusammen:

$$K,\ K^2,\ K^3,\ K^4,\ K^5 \ldots\ldots K^{(m)},\ K^{(m+1)},$$

so kehrt schließlich die Klasse K wieder; $K^{(m+1)} = K$.

Die Gesamtheit der Klassen K, K^2, K^3, K^4, K^5 .... $K^{(m)}$ nennt man mit Gauß (vgl. D. A. Art. 306 II) die Periode der Klasse K. Da das Quadrat eines Geschlechtes G von D das Hauptgeschlecht G_H, das Produkt aus diesem und G wiederum G ist, so werden in der Periode von K alle geraden Potenzen G_H, alle ungeraden dem Geschlechte G von K angehören. Die 3. Methode entwickelt nun die Periode einer Klasse K der negativen Determinante $-k \cdot M$ oder wenigstens ihren Anfang. Sie setzt dabei eine solche Klasse voraus, in deren zusammensetzender Form das Vorderglied eine möglichst kleine, in kM nicht aufgehende Primzahl ist.

Um einer solchen Zusammensetzung die allgemeine Grundlage zu geben, verfolgen wir zunächst diejenige einer Klasse K_1 mit den aufeinanderfolgenden Potenzen einer andern K_2 derselben Determinante, in deren zusammensetzenden Formen die Vorderglieder Potenzen derselben, in D nicht enthaltenen Primzahl sind. Jene seien

$$\text{in } K_1 \quad (a^\kappa,\ b,\ c), \qquad \text{in } K_2 \quad (a^\lambda,\ b',\ c').$$

Da sie im allgemeinen Falle nicht zusammensetzbar sind, müssen sie durch Formen ihrer Klassen von jener Eigenschaft ersetzt werden.

Gemäß der Voraussetzung gilt: $b^2 - b'^2 = (b - b')\ (b + b') = a^\kappa \cdot c - a^\lambda \cdot c'$. Nimmt man $\kappa \geqq \lambda$, so wird diese Gleichung durch a^λ teilbar. Da nun aber weder b, noch b′ durch a geteilt wird, muß entweder ihre Summe oder ihre Differenz durch a^λ teilbar sein.

1. $b + b'$ enthält a^λ als Faktor.

Dann $b + b' = a^\lambda \cdot g$ $\quad b' \equiv -b \pmod{a^\lambda}$. Der Form

$$(a^\lambda,\ b',\ c')$$

ist mithin diese $(a^\lambda, -b, c'')$ oder, da $c'' = \frac{b^2 - D}{a^\lambda} = c \cdot a^{\kappa-\lambda}$, die Form $(a^\lambda, -b, c \cdot a^{\kappa-\lambda})$ äquivalent. Ersetzt man ebenso die Form

$$(a^\kappa, b, c)$$

durch ihre äquivalente $(c, -b, a^\kappa)$, so sind die beiden Formen

$$(a^\lambda, -b, c \cdot a^{\kappa-\lambda}) \text{ und } (c, -b, a^\kappa)$$

zusammensetzbar und führen auf die zusammengesetzte Form:

$$(ca^\lambda, -b, a^{\kappa-\lambda}),$$

der diese $(a^{\kappa-\lambda}, b, c \cdot a^\lambda)$ äquivalent ist. Sie vertritt die aus K_1 und K_2 zusammengesetzte Klasse $K_1 \cdot K_2$.

$(ca^\lambda, -b, a^{\kappa-\lambda})$ setzt sich mit $(a^\lambda, -b, ca^{\kappa-\lambda})$ ohne weiteres zu

$$(ca^{2\lambda}, -b, a^{\kappa-2\lambda}),$$

der Kennform der Klasse $K_1 \cdot K_2^2$, diese mit $(a^\lambda, -b, ca^{\kappa-\lambda})$ zu

$$(ca^{3\lambda}, -b, a^{\kappa-3\lambda}),$$

einer Form der Klasse $K_1 \cdot K_2^3$ usf. zusammen.

Dieser einfache Algorithmus der Zusammensetzung, der die zusammengesetzten Formen aus der 1. Ausgangsform dadurch ableitet, daß er deren Mittelglied beibehält, dagegen ihr Vorderglied fortwährend um den Faktor a^λ schmälert und zum Hintergliede schlägt, wiederholt sich soviel Mal, als λ in κ enthalten ist. Ist

$$(h + 1)\,\lambda > \kappa > h \cdot \lambda,$$

so wird die letzte derartig zusammengesetzte Form $(a^{\kappa-h\lambda}, b, ca^{h\lambda})$ sein, die die Klasse $K_1\,K_2^h$ vertritt. Sie setzt sich mit $(ca^{\kappa-\lambda}, b, a^\lambda)$ zu $(c \cdot a^{2\kappa-\lambda(h+1)}, b, a^{(h+1)\lambda-\kappa})$, diese mit $(ca^{\kappa-\lambda}, b, a^\lambda)$ zu $(a^{(h+2)\lambda-\kappa}, -b, ca^{2\kappa-(h+2)\lambda})$, diese mit $(ca^{\kappa-\lambda}, b, a^\lambda)$ zu $(a^{(h+3)\lambda-\kappa}, -b, ca^{2\kappa-(h+3)\lambda})$ usf. zusammen.

Gilt $2(h + 1)\lambda > 2\kappa > (2h + 1)\lambda$, so gestattet auch das letzte Zusammensetzungsverfahren, das an der Form $(a^{(h+1)\lambda-\kappa}, -b, ca^{2\kappa-(h+1)\lambda})$ anhebt, die Mittelglieder der zusammengesetzten Formen zwar konstant hält, dagegen ihren Wert in den entgegengesetzten der obigen Formen verkehrt und ferner noch jedesmal zum Vordergliede a^λ hinzu-, vom Hintergliede wegnimmt, nur eine h fache Verwendung. Es endigt an der Form $(a^{(2h+1)\lambda-\kappa}, -b, c \cdot a^{2\kappa-(2h+1)\lambda})$, der repräsentativen Form der Klasse $K_1 \cdot K_2^{2h+1}$. Die weitere Zusammensetzung mit

$(a^\lambda, -b, ca^{\kappa-\lambda})$ oder die Fortsetzung der Reihe $K_1 \cdot K_2, K_1 \cdot K_2^2, K_1 \cdot K_2^3 \ldots . K_1 K_2^{2h+1}$ muß nunmehr nach der Methode des 2. Falles erfolgen, in welchen also schließlich der erste einmündet.

2. $b - b'$ ist teilbar durch a^λ.

Dann $b' \equiv b \pmod{a^\lambda}$; ferner (a^λ, b', c') äquivalent (a^λ, b, c'') oder, da wie in (1) $c'' = c \cdot a^{\kappa-\lambda}$, äquivalent $(a^\lambda, b, c \cdot a^{\kappa-\lambda})$. Da ihre Hinterglieder ihre Zusammensetzbarkeit stören, so können die beiden Formen (a^κ, b, c) und $(a^\lambda, b, c \cdot a^{\kappa-\lambda})$ nicht zusammengesetzt werden. Dazu muß (a^κ, b, c) in eine äquivalente Form desselben Vordergliedes übergeführt werden, deren Hinterglied durch a^λ teilbar wird. Sie habe das Mittelglied $b + f \cdot a^\kappa = B_1$. Zu dem Ende bemerkt man zunächst, daß die Wurzeln gleichen Vorzeichens der Kongruenz (A) nach den Moduln a^κ und $a^{\kappa+\lambda}$ bezüglich des ersteren einander kongruent sind. Da demnach $B_1 - b$ durch a^κ teilbar wird, wo B_1 die b entsprechende Wurzel bedeutet, so ist die lineare Kongruenz:

$$b + f \cdot a^\kappa \equiv B_1 \text{ oder } f \equiv \frac{B_1 - b}{a^\kappa} \pmod{a^{\kappa+\lambda}}$$

auflösbar. Demnach steht fest, daß es zu der Form (a^κ, b, c) eine äquivalente $(a^\kappa, B_1, a^\lambda \cdot C_1)$ der gewünschten Eigenschaften gibt. Die entsprechende Umformung von $(a^\lambda, b, ca^{\kappa-\lambda})$ führt auf $(a^\lambda, B_1, C_1 \cdot a^\kappa)$. Die beiden Formen

$$(a^\kappa, B_1, a^\lambda \cdot C_1) \text{ und } (a^\lambda, B_1, a^\kappa C_1)$$

gestatten nun ihre Zusammensetzung zu

$$(a^{\kappa+\lambda}, B_1, C_1),$$

einer Form der Klasse $K_1 \cdot K_2$. Ihre in obiger Weise geführte Zusammensetzung mit $(a^\lambda, B_1, a^\kappa \cdot C_1)$ ergibt $(a^{\kappa+2\lambda}, B_2, C_2)$, die Komposition dieser mit $(a^\lambda, B_2, a^{\kappa+\lambda} \cdot C_2)$ die Form $(a^{\kappa+3\lambda}, B_3, C_3)$ usf. Allgemein entwickelt man als Repräsentativform der Klasse $K_1 \cdot K_2^n$: $(a^{\kappa+n\lambda}, B_n, C_n)$.

Der einschlägige Fall verlangt die Zusammensetzung einer Klasse K mit ihren aufeinanderfolgenden Potenzen. Er spezialisiert sich aus dem allgemeinen durch

$$K = K_1 = K_2; \quad \kappa = \lambda = 1$$

Der Ausgangsform (a, b, c) von K sei die mit sich selbst zusammensetzbare Form $(a, B_2, a \cdot C_2)$ äquivalent. Durch Selbstkomposition geht sie über in (a^2, B_2, C_2), welche das Quadrat

K^2 der Klasse K vertritt. Sie setzt sich mit einer der Ausgangsform äquivalenten zu (a^3, B_3, C_3), diese mit einer äquivalenten von jener zu (a^4, B_4, C_4) usf. zusammen. Allgemein stellt (a^n, B_n, C_n) die aus jener Zusammensetzung herausentwickelte Form der Klasse K^n dar. In dieser Weise erschließt sich die Periode der Klasse K.

Was nun den Zusammenhang zwischen den Gliedern zweier aufeinanderfolgender Formen, allgemein dieser

$$(a^g, B_g, C_g) \text{ und } (a^{g+1}, B_{g+1}, C_{g+1})$$

betrifft, so ist derjenige ihrer Vorderglieder an und für sich klar. Ihre Mittelglieder stehen um ein Vielfaches von a^g auseinander:

$$B_{g+1} = B_g + f_g \cdot a^g.$$

Die Unbestimmte f_g geht aus der Beziehung ihrer Hinterglieder hervor; für C_{g+1} ergibt sich nämlich

$$C_{g+1} = \frac{(B_g + f_g \cdot a^g)^2 - B_g^2 + a^g C_g}{a^g \,.\, a} = \frac{f_g(f_g \,.\, a^g + 2B_g) + C_g}{a}$$

Sie verlangt, daß f_g der Kongruenz genügt: $2\, B_g \,.\, f_g \equiv -\, C_g$ (mod. a). Wenn a der Voraussetzung der Methode nachkommt, so begegnet die Auflösung jener Kongruenz und damit die Entwicklung der zusammengesetzten Formen keinen rechnerischen Schwierigkeiten.

Besondere Einfachheit zeichnet den Fall aus, in dem a sein Minimum 3 hat. f_g stehen dann nur die 3 Werte offen: 0, + 1 und — 1, von welchen der erste für ein durch 3 teilbares C_g, der zweite oder dritte statthat, je nachdem der Kongruenz

$$\pm 2 B_g \equiv -\, C_g \pmod 3$$

für das positive oder negative Vorzeichen genügt wird. Mithin ist, wobei die Nullen in den Klammern sich aufeinander beziehen,

$$B_{g+1} = B_g \pm 3^g(0)$$

$$C_{g+1} = 3^{g-1}(0) + \frac{C_g \pm 2 B_g(0).}{3}$$

Nachstehende Tabelle gibt das Muster zur Berechnung der zusammengesetzten Formen im Falle $a = 3$ unter Zugrundelegung der Ausgangsform $\left(3,\ 1,\ \frac{1+\Delta}{3}\right)$

1. $A = 3$	2. $B_1 = 1$	3. $C_1 = \frac{1+\Delta}{3}$
$A^2 = 9$	$B_2 = 1 \pm 3\,(0)$	$C_2 = 1\,(0) + \frac{C_1 \pm 2\,(0)}{3}$
$A^3 = 27$	$B_3 = B_2 \pm 9\,(0)$	$C_3 = 3\,(0) + \frac{C_2 \pm 2\,B_2\,(0)}{3}$
$A^4 = 81$	$B_4 = B_3 \pm 27\,(0)$	$C_4 = 9\,(0) + \frac{C_3 \pm 2\,B_3\,(0)}{3}$
$A^5 = 243$	$B_5 = B_4 \pm 81\,(0)$	$C_5 = 27\,(0) + \frac{C_4 \pm 2\,B_4\,(0)}{3}$

Dieser einfachste Fall bietet sich stets dar, sobald $k \cdot M \equiv 2\ (3)$ ist, was durch passende Wahl von k erreicht wird. Bedeutende Vereinfachung wird fernerhin dadurch erzielt, daß jede zusammengesetzte Form durch die einfachste ihrer Klasse, d. h. durch die ihr äquivalente reduzierte ersetzt wird.

Da die geraden Potenzen der Periode von K dem Hauptgeschlecht G_H von $-k \cdot M$ angehören, dieses aber die charakteristische Zahl 1 hat (vgl. den Hülfssatz auf S. 76), so werden alle Außenglieder der zugehörigen (reduzierten) Formen Reste von M darstellen. Weil ferner ihre ungeraden Potenzen demselben Geschlechte sich einordnen, so geben die Produkte aus zweien oder allgemein einer geraden Zahl Außenglieder ihrer reduzierten Formen Reste von M.

Fällt K selber in das Hauptgeschlecht, so trifft dies für die ganze Periode von K und mithin für sämtliche zusammengesetzten Formen zu; alle ihre Außenglieder sind Reste von M. Dieser Fall stellt sich ein, sobald es nach einer der beiden vorhergehenden Methoden gelungen ist, einen als a tauglichen Rest von $k \cdot M$ aufzudecken, der zudem noch den von $-k \cdot M$ vorgeschriebenen Spezialcharakter von G_H bezgl. 4 oder 8 einhält, also jedenfalls $\equiv 1\ (4)$ ist, falls $-k \cdot M \not\equiv 1\ (4)$. Denn da dann ein solches a den Totalcharakter von G_H angibt, so wird die Form (a, b, c) aus G_H stammen.

4. Methode.

Als eine 4. Methode zur Bestimmung tauglicher r läßt sich noch die Verallgemeinerung der ersten beifügen. Während diese nämlich M durch die besondern quadratischen Formen (a, o, c) darstellte, verwendet jene hierzu die allgemeinen Formen

(a, b, c). Grundbedingung der eigentlichen Darstellbarkeit von M durch (a, b, c) ist bekanntlich DRM, welche sich folgendermaßen ergibt. Gilt

$$M = a\alpha^2 + 2b\alpha\gamma + c\gamma^2,$$

so multipliziert man diese Gleichung hintereinander mit α und γ und erhält dadurch

$$(a\alpha + b\gamma)^2 = y^2 = D\gamma^2 + a \cdot M$$
$$(b\alpha + c\gamma)^2 = z^2 = D\alpha^2 + c \cdot M.$$

Diese beiden Gleichungen besagen, daß D quadratischer Rest aller derjenigen Primteiler von M ist, welche nicht in dem gemeinschaftlichen Teiler von α und γ aufgehn. Da aber auf Grund der eigentlichen Darstellbarkeit kein solcher besteht, muß D Rest aller Primteiler von M und damit von M selber sein. — Die Entwicklung von Formen (a, b, c), die M darstellen, kann auf folgende Weise vorgenommen werden. Man setzt $a = a_0$ und $x = x_0$ beliebig an und zerlegt hierauf die Differenz $M - a_0x_0^2$ in 2 Faktoren f_1 und f_2, von denen der eine y, der andere der Summe $2bx_0 + cy$ gleichgemacht wird, wobei x_0 und y relativ prim gehalten werden müssen. Es sei

$$y = f_1 \text{ und } 2bx_0 + cf_1 = f_2.$$

b und c gehen als ganzzahlige Lösungen der letzten unbestimmten Gleichung oder der Kongruenz

$$c \cdot f_1 \equiv f_2 \pmod{2x_0}$$

hervor. Es kommt offenbar darauf an, die Determinante D von (a, b, c) möglichst zu erniedrigen. Man kommt diesem Ziele wohl am nächsten, wenn mnn a_0 klein, x_0 dann so nimmt, daß die Differenz $M - a_0x_0^2$ wiederum klein ausfällt.

Indem $(ax + by)^2 - Dy^2 = a \cdot M$ ist, so erreicht diese Methode dasselbe wie die erste unter Anwendung auf das a-fache von M. Jedoch umgeht sie die Rechnung mit 7- oder noch-mehrstelligen Zahlen, welche den Tafelbereich der Quadratzahlen übersteigen.

An 3 Beispielen sollen die 4 Methoden ihren praktischen Wert beweisen.

1. $M = 857\,323.$

Die 1. Methode liefert:

$$M = 926^2 - 17 \cdot 3^2 =$$
$$= 2 \cdot 653^2 - 5 \cdot 17 \cdot 53 =$$

$$\begin{aligned} M &= 3\cdot 534^2 + 5\cdot 7\cdot 53 = \\ &= 3\cdot 535^2 - 2\cdot 26^2 = \\ &= 5\cdot 414^2 + 7\cdot 7^2 = \\ &= 6\cdot 378^2 + 19\cdot 1^2 = \\ &= 7\cdot 350^2 - 3\cdot 59 = \\ &= 11\cdot 279^2 + 67\cdot 4^2 = \\ &= 13\cdot 256^2 + 5\cdot 7\cdot 17\cdot 3^2 = \\ &= 13\cdot 257^2 - 2\cdot 73\cdot 3^2 \end{aligned}$$

Daraus gehen in gleicher Reihenfolge die Reste hervor: $+2\cdot 5\cdot 17\cdot 53$, $-3\cdot 5\cdot 7\cdot 53$, $+2\cdot 3$, $-5\cdot 7$, $-2\cdot 3\cdot 19$, $+3\cdot 7\cdot 59$, $-11\cdot 67$, $-5\cdot 7\cdot 13\cdot 17$, $+2\cdot 13\cdot 73$.

Die 2. Methode, die die Periode der Hauptklasse von $D = +857\,323$ entwickelt, ergibt:

(1, 925, — 1698); (— 1698, 773, 153); (153, 910, — 191); (— 191, 809, 1062); (1062, 253, — 747); (— 747, 494, 821); (821, 327, — 914); (— 914, 587, 561); (561, 535, — 1018); (— 1018, 483, 613); (613, 743, — 498); (— 498, 751, 589)

. . . . . .

Da sämtliche Außenglieder Reste darstellen, so kommen unter Entfernung der untauglichen zu jenen hinzu: $+153 = 9\cdot 17$, $+1062 = +2\cdot 9\cdot 59$, $-747 = -9\cdot 83$, $+561 = +3\cdot 11\cdot 17$, $-498 = -2\cdot 3\cdot 83$, $+589 = +19\times 31$.

Verbindet man die beiden Restkomplexe miteinander, so gelangt man zu den voneinander unabhängigen Resten:

$$+5, -6, -7, +13, +17, -19, -22, -31, -83.$$

Die Tafel I weist nur der Primzahl 701 diese Reste zu. In der Tat findet sich: $857\,323 = 701\cdot 1223$.

2. $M = 705\,937$.

Die 1. Methode zeigt an:

$$\begin{aligned} M &= 841^2 - 3\cdot 7\cdot (2^3)^2 = \\ &= 839^2 + 2\cdot 7\cdot (2^2\cdot 3)^2 = \\ &= 2\cdot 594^2 + 5\cdot 53\cdot 1^2 = \\ &= 2\cdot 593^2 + 7\cdot 13\cdot 29\cdot 1^2 = \\ &= 5\cdot 376^2 - 23\cdot 41\cdot 1^2 = \\ &= 5\cdot 375^2 + 19\cdot 37\cdot 2^2 = \\ &= 2\cdot 3\cdot 343^2 + 43\cdot 1^2 = \\ &= 7\cdot 319^2 - 2\cdot 5\cdot 71\cdot 3^2 = \\ &= 13\cdot 233^2 + 5\cdot (2\cdot 3)^2 = \\ &= 13\cdot 232^2 + 3\cdot 83\cdot 5^2 \end{aligned}$$

und damit die Reste:

$$+3\cdot7,\ -2\cdot7,\ -2\cdot5\cdot53,\ -2\cdot7\cdot13\cdot29,\ +5\cdot23\cdot41,$$
$$-5\cdot19\cdot37,\ -2\cdot3\cdot43,\ +2\cdot5\cdot7\cdot71,\ -5\cdot13,\ -3\cdot13\cdot83.$$

Die 3. Methode bildet die Periode einer Klasse mit der negativen Determinante $D = -k\cdot M$ ($k\cdot M \equiv 2 \pmod 3$).

Im vorliegenden Falle sei $k\cdot M = 1\,411\,874 = 2\cdot 705\,937$; das Vorderglied a der 1. Form = 3. Sonach kommt unter Beobachtung des auf S. 82 angegebenen Algorithmus:

$C^1 = (3, 1, 470625)$	$C^2 = (9, 1, 156875)$
$C^3 = (27, -8, 52294)$	$C^4 = (81, 19, 17435)$
$C^5 = 243), -62, 5826)$	$C^6 = (729, -62, 1942)$
$C^7 = (849, 182, 1709)$	$C^8 = (283, -101, 5025)$
$C^9 = (849, -101, 1675)$	$C^{10} = (774, 26, 1825)$
$C^{11} = (258, 26, 5475)$	$C^{12} = (86, 26, 16425)$
$C^{13} = (258, 112, 5521)$	$C^{14} = (774, 370, 2001)$
$C^{15} = (667, 297, 2249)$	$C^{16} = (1170, 206, 1243)$
$C^{17} = (390, -184, 3707)$	$C^{18} = (130, -54, 10883)$
$C^{19} = (390, 76, 3635)$	$C^{20} = (1170, -314, 1291)$

Daraus fließen die Reste:

aus C^8 $3\cdot67$, aus C^{10} $2\cdot43$ und 73, aus C^{14} $3\cdot23\cdot29$, aus C^{15} $3\cdot13\cdot173$, aus C^{16} $2\cdot5\cdot13$ und $11\cdot113$.

Die Kombination dieser Reste mit den vorhergehenden gibt folgende unabhängige Reste an die Hand:

$$-1,\ 2,\ 3,\ 7,\ 43,\ 65,\ 67,\ 73.$$

Auf Grund der 4 ersten müssen die Primfaktoren von 705 937 in eine der Formen

$$168\,x + 1,\ 25,\ 121$$

eingehen. Unter den 169 Primzahlen bis 1000 haben nur 4 diese Gestalt, abgesehen von 1, nämlich: 193, 237, 457 und 673, welche aber M nicht teilen. Indem es also gelungen ist, den Komplex Ω bis auf 4 Glieder zu erniedrigen, ist die Tafel I entbehrlich geworden. Sie bestätigt aber auch, daß M = 705 937 prim ist.

3. M = 998 581.

Die 1. Methode wird insofern abgeändert, als M nicht mehr konstant gehalten wird, sondern an seine Stelle hintereinander seine 20 ersten Vielfachen treten. Zu jedem derselben werden die beiden Quadrate bestimmt, welche es einschließen,

und ihre Differenzen von ihm, welch letztere Reste von M liefern.

$1\,000\,000 = 1\,000^2$	$1\,419 = 3 \cdot 11 \cdot 43$
$998\,581 = 1 \cdot M$	
$998\,001 = 999^2$	$-\ 580 = -\ 4 \cdot 5 \cdot 19$
$1\,999\,396 = 1\,414^2$	$2\,234 = 2 \cdot 1\,117$
$1\,997\,162 = 2 \cdot M$	
$1\,996\,569 = 1\,413^2$	$-\ 593$
$2\,996\,361 = 1\,731^2$	$618 = 2 \cdot 3 \cdot 103$
$2\,995\,743 = 3 \cdot M$	
$2\,992\,900 = 1\,730^2$	$-\ 2\,843$
$3\,996\,001 = 1\,999^2$	$1\,677 = 3 \cdot 13 \cdot 43$
$3\,994\,324 = 4 \cdot M$	
$3\,992\,004 = 1\,998^2$	$-\ 2\,320 = -\ 2^2 \cdot 5 \cdot 29$
$4\,995\,225 = 2\,235^2$	$+\ 2\,320 = 2^2 \cdot 5 \cdot 29$
$4\,992\,905 = 5 \cdot M$	
$4\,990\,756 = 2\,234^2$	$-\ 2\,149 = -\ 7 \cdot 307$
$5\,992\,704 = 2\,248^2$	$1\,218 = 2 \cdot 3 \cdot 7 \cdot 19$
$5\,991\,486 = 6 \cdot M$	
$5\,987\,809 = 2\,247^2$	$-\ 3\,677$
$6\,990\,736 = 2\,644^2$	$669 = 3 \cdot 223$
$6\,990\,067 = 7 \cdot M$	
$6\,985\,449 = 2\,643^2$	$-\ 4\,618 = 2 \cdot 2309$
$7\,991\,929 = 2\,827^2$	$3\,281 - 17 \cdot 193$
$7\,988\,648 = 8 \cdot M$	
$7\,986\,276 = 2\,826^2$	$-\ 2\,372 = -\ 2^2 \cdot 593$
$8\,988\,004 = 2\,998^2$	$775 = 31 \cdot 5^2$
$8\,987\,229 = 9 \cdot M$	
$8\,982\,009 = 2\,997^2$	$-\ 5\,220 = -\ (2 \cdot 3)^2 \cdot 5 \cdot 29$
$9\,991\,921 = 3\,161^2$	$6\,111 = 7 \cdot 97 \cdot 3^2$
$9\,985\,810 = 10 \cdot M$	
$9\,985\,600 - 3\,160^2$	$-\ 210 = -\ 2 \cdot 3 \cdot 5 \cdot 7$
$10\,989\,225 = 3\,315^2$	$4\,834 = 2 \cdot 2\,417$
$10\,984\,391 = 11 \cdot M$	
$10\,982\,596 = 3\,314^2$	$-\ 1\,795 = -\ 5 \cdot 359$
$11\,985\,444 = 3\,462^2$	$2 \cdot 3 \cdot 103 \cdot 2^2$
$11\,982\,972 = 12 \cdot M$	
$11\,978\,621 = 3\,461^2$	$-\ 4\,351 = -\ 19 \cdot 229$
$12\,981\,609 = 3\,603^2$	$56 = 2^3 \cdot 7$
$12\,981\,553 = 13 \cdot M$	
$12\,974\,404 = 3\,602^2$	$-\ 7\,149 = -\ 3 \cdot 2\,383$
$13\,987\,600 = 3\,740^2$	$7\,466 = 2 \cdot 3\,733$
$13\,980\,134 = 14 \cdot M$	
$13\,980\,121 = 3\,739^2$	$-\ 13$

$14\,984\,641 = 3\,871^2$ $14\,978\,715 = 15 \cdot M$ $14\,976\,900 = 3\,870^2$	$5\,926 = 2 \cdot 2\,963$ $-1\,815 = -3 \cdot 5 \cdot 11^2$
$15\,984\,004 = 3\,998^2$ $15\,977\,296 = 16 \cdot M$ $15\,976\,009 = 3\,997^2$	$6\,708 = 2^2 \cdot 3 \cdot 13 \cdot 43$ $-1\,287 = -3^2 \cdot 11 \cdot 13$
$16\,982\,641 = 4\,121^2$ $16\,975\,877 = 17 \cdot M$ $16\,974\,400 = 4\,120^2$	$6\,764 = 2^2 \cdot 19 \cdot 89$ $-1\,477 = -7 \cdot 211$
$17\,977\,600 = 4\,353^2$ $17\,974\,458 = 18 \cdot M$ $17\,969\,121 = 4\,239^3$	$3\,142 = 2 \cdot 1\,571$ $-5\,337 = -3^2 \cdot 593$
$18\,974\,736 = 4\,356^2$ $18\,973\,039 = 19 \cdot M$ $18\,966\,025 = 4\,355^2$	$1\,697$ $-7\,014 = -2 \cdot 3 \cdot 7 \cdot 167$
$19\,971\,961 = 4\,469^2$ $19\,971\,620 = 20 \cdot M$ $19\,963\,024 = 4\,468^2$	$341 = 11 \cdot 31$ $-8\,596 = -2^2 \cdot 7 \cdot 307$

Die 4. Methode bewirkt für $a_0 = 5$ folgendes:

$998\,581$ $972\,405$ $= 5 \cdot 441^2$	$f_1 \cdot f_2 = 26\,176$ $f_1 = 4,\ f_1 = 6544$	$4c \equiv 6\,544 \pmod{882}$; $2c \equiv 3\,272 \pmod{411}$ $c = 185$ $D = 49 - 5 \cdot 185 = -2^2 \cdot 3 \cdot 73$
$4\,415$ $976\,820$ $= 5 \cdot 442^2$	$4\,415$ $f_1 f_2 = 21\,761$ $f_1 = 1,\ f_2 = 21\,761$	$c \equiv 21\,716 \pmod{884}$ $c = 545$ $D = 576 - 5 \cdot 545 = -7 \cdot 307$
$4\,425$ $980\,245$ $= 5 \cdot 443^2$	$4\,425$ $f_1 f_2 = 17\,336$ $f_1 = 4;\ f_2 = 4334$	$2c \equiv 2\,167 \pmod{443}$ $c = 419$ $D = 9 - 5 \cdot 419 = -2 \cdot 7 \cdot 149$
$4\,435$ $985\,680$ $= 5 \cdot 444^2$	$4\,435$ $f_1 f_2 = 12\,901$ $f_1 = 7,\ f_2 = 1843$	$7c \equiv 1\,843 \pmod{888}$ $c = -371$ $D = 9 + 5 \cdot 371 = 2^3 \cdot 233$
$4\,445$ $990\,125$ $= 5 \cdot 445^2$	$4\,445$ $f_1 f_2 = 8\,456$ $f_1 = 4,\ f_2 = 2 \cdot 1057$	$2c \equiv 1\,057 \pmod{890}$ $c = -139$ $D = 9 + 5 \cdot 139 = 2^6 \cdot 11$
$4\,455$ $994\,580$ $= 5 \cdot 446^2$	$4\,455$ $f_1 f_2 = 4\,001$ $f_1 = 1,\ f_2 = 4001$	$c \equiv 4\,001 \pmod{892}$ $c = -459$ $D = 5 \cdot 5 + 5 \cdot 459 = 2^4 \cdot 5 \cdot 29$
$4\,465$ $999\,045$ $= 5 \cdot 447^2$	$4\,465$ $f_1 f_2 = -464$ $f_1 = 8,\ f_2 = -58$	$8c \equiv -58 \pmod{894}$ $c = -119$ $D = 1 + 5 \cdot 119 = 2^2 \cdot 149$
$4\,475$ $1\,003\,520$ $= 5 \cdot 448^2$	$4\,475$ $f_1 f_2 = -4\,939$ $f_1 = 11,\ f_2 = 449$	$11c \equiv -449 \pmod{896}$ $c = -611$ $D = 49 + 5 \cdot 611 = 2^5 \cdot 97$

$4\,485$ $1\,008\,005$ $= 5 \cdot 449^2$	$4\,485$ $f_1 \cdot f_2 = -9\,424$ $f_1 = 8,\ f_2 = -1178$	$4c \equiv -589 \pmod{449}$ $c = 1\,312$ $D = 169 - 5 \cdot 1312 = -7 \cdot 11 \cdot 83$
$4\,495$ $1\,012\,500$ $= 5 \cdot 450^2$	$4\,495$ $f_1 \cdot f_2 = -13\,919$ $f_1 = 31,\ f_2 = -449$	$31c \equiv -449 \pmod{900}$ $c = 421$ $D = 225 - 5 \cdot 421 = 2^3 \cdot 5 \cdot 47$
$4\,505$ $1\,017\,005$ $= 5 \cdot 451^2$	$4\,505$ $f_1 \cdot f_2 = -18\,424$ $f_1 = 4,\ f_2 = 4\,606$	$2c \equiv -2\,303 \pmod{451}$ $c = 878$ $D = 81 - 5 \cdot 878 = -31 \cdot 139$
$4\,515$ $1\,021\,520$ $= 5 \cdot 452^2$	$4\,515$ $f_1 f_2 = -22\,939$ $f_1 = 7,\ f_2 = -3277$	$7c \equiv -3\,277 \pmod{904}$ $c = -339$ $D = 1 + 5 \cdot 339 = 2^5 \cdot 53$

Zusammenstellung der Reste beider Methoden:

$+ 3 \cdot 11 \cdot 43, -5 \cdot 19, + 2 \cdot 3 \cdot 103, + 3 \cdot 13 \cdot 43, -5 \cdot 29, + 5 \cdot 29, -7 \cdot 307, + 2 \cdot 3 \cdot 7 \cdot 19, + 3 \cdot 223, + 17 \cdot 193, + 31, + 7 \cdot 97, -2 \cdot 3 \cdot 5 \cdot 7, -5 \cdot 359, + 2 \cdot 3 \cdot 103, -19 \cdot 229, + 2 \cdot 7, -13, -3 \cdot 5, + 3 \cdot 13 \cdot 43, -11 \cdot 13, + 19 \cdot 89, -7 \cdot 211, -6 \cdot 7 \cdot 167, + 11 \cdot 31, -7 \cdot 307; + 149, + 5 \cdot 29, + 11, + 2 \cdot 233, -2 \cdot 7 \cdot 149, -7 \cdot 307, -3 \cdot 73, + 2 \cdot 97, -7 \cdot 11 \cdot 83, + 2 \cdot 5 \cdot 47, -31 \cdot 139, + 2 \cdot 53.$

Aus ihnen zieht man die voneinander unabhängigen Reste:

$$-1, 11, 13, 14, 15, 31, 57, 87, 95,$$

welche im Bereiche der Tafel I nur die Primzahl 113 besitzt. Demnach ist 113 in 998 581 enthalten:

$$998\,581 = 113 \cdot 8837.$$

Da die Primteiler des zweiten Faktors 8837 mit dem Produkte in jenen Resten übereinstimmen, mithin mindestens einer durch die Tafel angezeigt werden müßte, so folgt, daß 8837 ebenfalls prim ist.

2. Methode von Gauß zur Primzahlbestimmung.

Ihr Prinzip.

Zur Bestimmung des primen oder zusammengesetzten Charakters von M dient die Wurzelanzahl der Kongruenz (A) (vgl. S. 11). Ist nämlich M prim oder primäquivalent (vgl. S. 13), so besitzt (A) 2 entgegengesetzte (mod. M) inkongruente Wurzeln; setzt sich aber M aus μ ungeraden Primteilern in beliebigen Potenzen zusammen, so genügen (A) 2^μ (mod. M) inkongruente

Wurzeln. Dadurch steht ein Weg zur Unterscheidung primer und zusammengesetzter Zahlen offen.

Wurzelbestimmung von (A).

Sie benützt den Satz, daß jede eigentliche Darstellung von M zu einer Wurzel von (A) gehört. Die Formen mit der Determinante D, welche M darstellen, werden folgenden äquivalent sein:

$$(\alpha)\quad \begin{matrix}(M, & n_1, m_1), (M, & n_2, m_2) \ldots\ldots\ldots\ldots (M, & n_l, m_l),\\ (M, & -n_1, m_1), (M, & -n_2, m_2) \ldots\ldots\ldots\ldots (M, & -n_l, m_l),\end{matrix} \quad l = 2^{\mu-1},$$

wo die Werte n und m in der Bedeutung von S. 13 wiederkehren. Jede der Formen (α) repräsentiert eine Klasse von D. Es können sich mithin 2^μ derselben an der Darstellung von M beteiligen. Möglichenfalls werden sie jedoch teilweise oder gänzlich in eine einzige zusammenfallen. Aus sämtlichen Klassen (A) von D, die M darstellen, zieht man also sämtliche Wurzeln von (A).

Ist nun M prim zu 2D, eine Bedingung, der sich die untersuchte Zahl stets unterwirft, so werden alle Klassen (A), die sich zunächst der Kenntnis entziehen, einem einzigen eigentlich primitiven Geschlecht (𝔄) von D angehören, dessen Totalcharakter M angibt (vgl. S. 48). Die Klassen (A) werden unter denen von (𝔄) enthalten sein. Treten für diese ihre einfachsten Formen $f_1, f_2 \ldots\ldots f_n$ ein, so sucht man alle Darstellungen von M durch $f_1, f_2 \ldots\ldots f_n$.

Allgemein gehört dann zu einer Darstellung (x, y) von M durch f = (a, b, c) eine Wurzel n, die die beiden Kongruenzen befriedigt

$$(B):\ ax + by + ny \equiv bx + cy - nx \equiv 0 \pmod{M}.$$

Je nachdem aus den Darstellungen ein oder mehrere Paare entgegengesetzter Wurzeln der Kongruenz (A) hervorgehen, kündet sich M als prim, bzw. primäquivalent oder als zusammengesetzt an. Der Darstellungen von M versichert man sich durch die Ausschließungsmethode (vgl. D. A. 323—326), welche unmittelbare Anwendung auf alle quadratische Formen mit positiven Außen- und verschwindendem Mittelgliede gestattet. Jedoch läßt sich auf eine solche jede andere mit negativer Determinante ohne Änderung derselben bringen (vgl. Schluß von 326). Jene liefert hiernach nicht die Darstellungen von M selber,

sondern i. A. eines Vielfachen von M, aus denen aber die ersteren ohne weiteres abgeleitet werden.

Fingerzeige zur Wurzelbestimmung von (A).

1. Sie erreicht ihre größte Einfachheit, wenn das Geschlecht $\mathfrak{A}$ möglichst wenig Klassen umfaßt und somit nur eine geringe Zahl von Formen f zur Darstellung von M herangezogen werden muß. Der günstigste Fall ist also der, daß D der Reihe der $65\,D_1$ (vgl. S. 48) angehört, die in ihren eigentlich primitiven Geschlechtern nur je eine Klasse enthalten. Dann muß eine einzige Form f M zu sämtlichen Wurzeln von (A) gehörig darstellen. Umfassen die eigentlich primitiven Geschlechter von D je 2 oder 3 Klassen, so können sich die Darstellungen von M auf 2 oder 3 Formen f verteilen u. s. f.

2. Einschränkung in der Zahl der zu untersuchenden Klassen von $\mathfrak{A}$.

Jedes Geschlecht zerfällt in nichtambige und ambige Klassen, jene wieder in Paare entgegengesetzter Klassen. Wie schon auf S. 13 hervorgehoben, stellen 2 entgegengesetze Klassen dieselben Zahlen zu entgegengesetzten Wurzeln von (A) gehörig dar. Durch die Wurzeln, welche irgend eine nichtambige Klasse liefert, sind also diejenigen der entgegengesetzten Klasse mitbestimmt. Mithin fällt die eine Hälfte der nichtambigen Klassen für die Wurzelentwicklung fort. Eine ambige Klasse ist sich selbst entgegengesetzt. Jede ihrer Formen stellt dieselbe Zahl zu entgegengesetzten Wurzeln von A dar. Damit wiederholt sich auch an den ambigen Klassen, daß die mit ihnen verbundenen Wurzeln von (A) sich paarweis bestimmen.

Einschränkung der Zahl der noch übrigbleibenden Darstellungen.

Nach S. 11 entfallen, abgesehen von $D = -1$, auf eine Wurzel von (A) 2 Darstellungen $\begin{pmatrix} x, & y \\ -x, & -y \end{pmatrix}$; mithin kann die Hälfte jener übergangen werden. Was den Fall $D = -1$ betrifft, so ordnen sich die Formen dieser Determinante in eine einzige eigentlich primitive Klasse mit (1, 0, 1) als einfachster Form ein. Zu einem entgegengesetzten Wurzelpaar gehören, wie S. 13 lehrt, 8 Darstellungen, die sich aber nur durch Vorzeichen und Reihenfolge der Unbestimmten unterscheiden. Da aber eine beliebige unter ihnen jenes übermittelt, so braucht nur der 8. Teil

sämtlicher Darstellungen von M durch (1, 0, 1) zur Wurzelentnahme verwandt zu werden.

Faktorenbestimmung von M mittels der Wurzeln von (A).

Genügen der Kongruenz (A) 2^{μ} (mod. M) inkongruente Wurzeln, so setzt sich M aus μ Primzahlpotenzen zusammen, zu denen man auf folgendem Wege gelangt. Setzt man $M = p_1^{\alpha_1} p_2^{\alpha_2} \ldots . p_{\mu}^{\alpha_{\mu}}$ und löst (A) in μ Kongruenzen nach den Primzahlpotenzen p^{α} als Moduln auf, so kommt:

(A_1): $r_1^2 \equiv D$ (mod. $p_1^{\alpha_1}$) (A_2): $r_2^2 \equiv D$ (mod. $p_2^{\alpha_2}$) (A_3): $r_3^2 \equiv D$ (mod. $p_3^{\alpha_3}$) . . . . . (A_{μ}): $r_{\mu}^2 \equiv D$ (mod. $m_{\mu}^{\alpha_{\mu}}$).

Bedeuten allgemein $\pm r_i$ die beiden Wurzeln von (A_i), so erhellt, daß die Wurzeln n alle gemeinsamen Lösungen des Kongruenzensystemes:

$$n \equiv \pm r_1 \text{ (mod. } p_1^{\alpha_1}) \equiv \pm r_2 \text{ (mod. } p_2^{\alpha_2})$$
$$\equiv \pm r_3 \text{ („ } p_3^{\alpha_3}) \ldots \equiv \pm r_{\mu} \text{ („ } p_{\mu}^{\alpha_{\mu}})$$

darstellen. Da die feste Wurzel n_1 den übrigen nach den Primzahlpotenzen und deren Produkten bezw. kongruent ist, so müssen die Differenzen aus jenen diese der Reihe nach als Faktoren enthalten. Bildet man zunächst die Differenzen aus $+ n_1$ und $+ n_1$, $- n_1$, so hat die erste $n_1 - n_1$ mit M den Teiler M, die zweite $n_1 + n_1$ mit M den Teiler 1 gemein. Jede andere Differenz $n_1 - n_i$ kann weder prim zu M noch ein Vielfaches von M sein, sondern hat mit M mindestens eine Primzahlpotenz p^{α} gemein. Da $n_1^2 - n_i^2 = (n_1 - n_i)(n_1 + n_i)$ durch $M = M' \cdot M''$ geteilt wird, so ist, falls M' in $(n_1 - n_i)$ aufgeht, M'' in $(n_1 + n_i)$ oder in der Differenz $n_1 - (- n_i)$ enthalten. Übrigens läßt sich die Faktorenbestimmung von M ohne Kenntnis der Wurzeln n durchführen. Unter Benützung der Kongruenzen (B) (vgl. S. 89) folgt:

$$\begin{array}{l|l} n_1 \cdot x_1 \equiv bx_1 + cy_1 \equiv x_1' & x_i \\ n_i \cdot x_i \equiv bx_i + cy_i \equiv x_i' & x_1 \end{array} \quad \text{(mod. M)}$$

Multipliziert man die erste Kongruenz mit x_i, die zweite mit x_1 und subtrahiert diese von jener, so kommt:

$$x_1 \cdot x_i (n_1 - n_i) \equiv x_i \cdot x_1' - x_1 \cdot x_i' \text{ (mod. M).}$$

Demnach teilt der größte gemeinsame Faktor M' von M und $n_1 - n_i$ auch die Differenz $x_i \cdot x_1' - x_1 \cdot x_i'$, somit kann M' auch

dieser entnommen werden. Zur Feststellung der Teiler von M bedarf es also nur der Bildung aller Differenzen

$$x_i \cdot x_1' - x_1 \cdot x_i';$$

jene sind unter den Faktoren von diesen enthalten.

Die beiden Voraussetzungen der 2. Methode.

1. Die Auflösbarkeit der Kongruenz (A) diente als Grundlage der vorhergehenden Ausführungen. Sie wird auch von Gauß zunächst angenommen, d. h. es wird von vorneherein M der quadratische Rest D zugewiesen:

$$\left(\frac{D}{M}\right) = + 1.$$

Negative quadratische Reste von M gibt die 1. Methode an die Hand. Unter diesen werden diejenigen herausgegriffen, deren eigentlich primitive Geschlechter möglichst wenig Klassen enthalten. Von größtem Vorteil ist es, wenn ein Rest D_1 sich einstellt. Auf jeden Fall liefert das Geschlecht $\mathfrak{A}$, das M bestimmt, Darstellungen von M und damit die Wurzeln von (A), woraus gemäß dem Eingang S. 13 auf ein primes oder zusammengesetztes M geschlossen wird.

2. Die andere Voraussetzung zur 2. Methode macht diese von der ersten unabhängig: M hat nicht mehr den Rest D ($D < 0$), sondern kommt nur noch in den Teilerformen von D vor, in die die Hälfte aller zu (2) D primen Zahlen eingeht. M nimmt also eine Form

$$(4) c \cdot D + r$$

an, in der c einen laufenden Koeffizienten bezeichnet und r nach den Vorschriften der D. A. Art. 147—150 bestimmt wurde. M braucht nun nicht den Rest D zu besitzen, sondern es steht nur soviel fest, daß eine gerade Anzahl ungerader Primteiler von M in dem Nichtreste D übereinstimmt, wobei die Null auch als gerade Zahl gerechnet wird. M gibt dann einen zulässigen Totalcharakter von D an (vgl. D. A. Art. 263). Diesem muß, wie Gauß mit Hülfe der Theorie der ternären quadratischen Formen zeigt, ein eigentlich primitives Geschlecht $\mathfrak{A}$ von D entsprechen. Übrigens folgt diese Beziehung ohne weiteres aus dem Satze über die arithmetische Progression (vgl. dazu: Vorlesungen über Zahlentheorie von Dirichlet S. 328).

Man erschließt nun die Darstellungen von M durch die einfachsten Formen $f_1, f_2 \ldots$ der Klassen von $\mathfrak{A}$ und daraus die Wurzeln von (A). Finden gar keine Darstellungen von M statt, so bekundet sich damit D als Nichtrest von M, und M kann weder eine Primzahl, noch eine ungerade Potenz einer solchen sein. Um in solchem Falle die Faktoren von M zu finden, muß man entweder ein anderes Verfahren einschlagen oder das vorige an einem solchen Wert von D wiederholen, der sich schließlich als Rest von M herausstellt. Wiederum gebietet die Kürze der Rechnung, D der Reihe der 65 D_1 und zwar den größten zu entnehmen, einerseits weil dadurch die Klassenzahl κ von $\mathfrak{A} = 1$ wird, und andrerseits weil große Determinanten die Gaußsche Ausschließungsmethode (vgl. S. 89) beschleunigen. Man wählt demnach zuerst D = — 1848, dann = — 1365, — 1320, — 840 usw.

Erst wenn kein D_1 sich eignet, d. h. wenn M in den Nichtteilerformen sämtlicher D_1 erscheint, wird man zu den Determinanten D_2 mit zweiklassigen eigentlich primitiven Geschlechtern übergehen. Gauß gibt die Wahrscheinlichkeit jenes Ereignisses zu $\frac{1}{16384} = \frac{1}{2^{14}}$ an (vgl. Art. 334 II). In der Tat bedingt es, daß M auch in den Nichtteilerformen der 14 Primteiler auftritt, die die 65 D_1 zusammensetzen. Da nun gleich viel Teiler- und Nichtteilerformen desselben Moduls vorhanden sind, so ist die Wahrscheinlichkeit, daß M eine Nichtteilerform einer jener Primzahlen hat, $= \frac{1}{2}$, diejenige, daß M eine solche jeder derselben besitzt, $= \frac{1}{2^{14}}$.

Uneigentliche Darstellungen von M.

Die Bedingung ihrer Möglichkeit ist in erster Linie, daß M mindestens einen quadratischen Faktor enthält; jedoch nicht diese, daß D Rest des ganzen M ist. Sie sind mit keiner Wurzel von (A) verbunden und können folglich die Wurzelbestimmung von (A) nicht fördern. Immerhin zeigen sie einen quadratischen Teiler von M an und widerlegen somit ein primes M. Alle Quotienten Q aus M und seinen quadratischen Teilern tragen den gleichen Totalcharakter wie M; somit werden sie, wenn dies von M gilt, ebenfalls durch das Geschlecht $\mathfrak{A}$ eigentlich dargestellt, und man erkennt, daß nur dieses zu sämtlichen

eigentlichen und uneigentlichen Darstellungen von M befähigt ist. Um die zweite Bedingung für das Auftreten uneigentlicher Darstellungen zu erkennen, hält man nach den obigen beiden Voraussetzungen auseinander.

1. D ist Rest von M; dann ist D auch Rest sämtlicher Faktoren von M und mithin der Q. M wird dann durch $\mathfrak{A}$ soviel Mal uneigentlich dargestellt, als die Quotienten Q zusammen es eigentlich werden. Ist D gleich einem D_1, so muß eine einzige Form f sämtliche eigentlichen und uneigentlichen Darstellungen von M liefern, deren Anzahl die Formel auf S. 18 ausdrückt.

2. M hat eine Teilerform von D. Dann ist D Nichtrest einer geraden Zahl Primteiler p_n von M, von den übrigen p_r Rest. Wird nun mindestens ein Quotient Q nur aus den p_r gebildet, so wird dieser durch $\mathfrak{A}$ eigentlich und somit M uneigentlich dargestellt. Im andern Falle sind sowohl eigentliche, als auch uneigentliche Darstellungen von M ausgeschlossen. — Auch die uneigentlichen Darstellungen von M gehen durch die Ausschließungsmethode hervor; vor allem stellt diese unter Anwendung der Hauptform $(1, 0, \Delta)$, welche dann selber zu den Formen f zählt, ein quadratisches M fest. Somit ergibt sich: Wird M durch D weder eigentlich, noch uneigentlich dargestellt, so ist M sicherlich keine Primzahlpotenz.

Bemerkungen zur Gaußschen Methode.

Da M einen zulässigen Totalcharakter von D angibt, falls es in den Teilerformen von D vorkommt, und umgekehrt, so kann man von M anstatt dieser jenen fordern. Einer Determinante, die zur Primzahlbestimmung dienen soll, ordnet man also zweckmäßig das System aller ihrer zulässigen Totalcharaktere zu. Nimmt die zu untersuchende Zahl M einen derselben an, so lassen sich durch das diesem zugehörige Geschlecht $\mathfrak{A}$ Darstellungen von M erwarten. Gibt die Hülfsform $\left(\delta, 0, \frac{\Delta}{\delta}\right)$, in welche man eine einfache Form $f = (a, b, c)$ von $\mathfrak{A}$ transformiert hat, zwei oder mehr Zerlegungen von $a' \cdot M$; wo $a = a'\delta$, $b = b'\delta$ angenommen, so reichen diese zur Bestimmung der Faktoren von $a'M$ und damit von M, falls solche überhaupt vorhanden, nach dem Verfahren von S. 22 aus. Sonach lassen sich in diesem Falle, der für die $65\,D_1$ ausschließlich gilt, die

Darstellungen von M durch $\mathfrak{A}$, aus welchen Gauß (vgl. oben) die Faktoren von M hergeleitet hat, umgehen.

Erweiterungen der Gaußschen Methode.

Obgleich theoretisch auf alle Determinanten, so kann schlechthin die Gaußsche Methode praktisch nur auf die 65 D_1 Anwendung finden. Für diese ist der etwaige Darstellungsbereich von M auf eine einzige Klasse und somit auf eine einzige reduzierte Form beschränkt; sie ersparen also die Wiederholungen der Methode. Gauß nimmt in der Tat für seine Methode nur die 65 D_1 in Anspruch. Als Erweiterungen derselben sollen mithin ihre Ausdehnungen auf andere, d. h. auf mehrklassige Determinanten bezeichnet werden.

Welche Determinanten stellen sich fernerhin zur Verfügung, ohne zuviel Rechnungsarbeit aufzubürden? Von vorneherein sind es diejenigen, die, abgesehen von den D_1, in ihren eigentlich primitiven Geschlechtern möglichst wenig, d. h. nur 2, 3 oder 4 Klassen enthalten. 2 verschiedene Wege sind schon zu ihrer Anwendung eingeschlagen worden:

1. Durch Seelhoff.

Dieser benützt in seiner schon erwähnten Arbeit zur Primzahlbestimmung außer den 65 D_1 noch 105 andere, teils zwei-, teils vierklassige Determinanten; jedoch von diesen nur solche Geschlechter, die vollständig aus ambigen Klassen bestehen und die wir kurz ambig nennen werden im Gegensatze zu nichtambigen Geschlechtern, die nur nichtambige Klassen enthalten. Da ferner die reduzierten Formen jener Geschlechter sämtlich das Mittelglied ausstoßen und somit die unmittelbare Anwendung der Ausschließungsmethode gestatten, kann er statt eines Vielfachen von M die Zahl M selber untersuchen. Einteilungsgrund der Determinanten bilden nicht diese selber, sondern ihre Totalcharaktere derart, daß zu jedem derselben die Determinanten samt ihren reduzierten Formen gestellt werden, die in ihm übereinstimmen, demnach eine und dieselbe Determinante so oft wiederkehrt, als Geschlechter aus ihr entnommen worden sind.

2. Durch Pepin.

Dieser geht von dem schon einmal (vgl S. 51) herangezogenen Satz aus, daß die Klassenzahl κ der Geschlechter der

negativen Determinanten von der Form $8n + 5$ oder $-(8n + 3)$ stets durch 3 teilbar ist (vgl. D. A. Art. 256 VI). Unter diesen finden sich mindestens 17, für welche $\kappa = \mathbf{3}$ ist; ihre absolut kleinste ist -163, ihre absolut größte -1435. Das Hauptgeschlecht G_H derselben wird durch die 3 reduzierten Formen vertreten:

$$(1, 0, 8n + 3), (4, +1, 2n + 1), (4, -1, 2n + 1).$$

Trägt also M den Totalcharakter von G_H, d. h. ist M Rest aller ungeraden Primteiler des zugehörigen D, so ist M a priori durch G_H darstellbar. Beteiligen sich daran nur die beiden entgegengesetzten Formen von G_H, so wird aber notwendig 4 M durch $(1, 0, 8n + 3)$ zur Darstellung gelangen. Mithin sucht er allgemein Darstellungen von 4 M durch die Hauptform von G_H. Der Pepinschen Methode haftet offenbar der Nachteil geringer Verwendbarkeit an.

3. Eine dritte Erweiterung des Gaußschen Verfahrens, die die vorhergehende in sich begreift und in der Theorie sich auf Determinanten mit beliebig vielen Klassen in den eigentlich primitiven Geschlechtern erstreckt, besteht in folgendem. Unter der Voraussetzung, daß M prim zu 2D ist, wird M ausschließlich durch das eigentlich primitive Geschlecht $\mathfrak{A}$ eigentlich und uneigentlich dargestellt. Es bedeute nun m die kleinste Zahl, die durch sämtliche Klassen von $\mathfrak{A}$ eigentliche oder uneigentliche Darstellungen erfährt. Letztere gehen auf eigentliche Darstellungen der Quotienten aus m und seinen quadratischen Teilern zurück, soweit ihr Darstellungsbereich in das Geschlecht $\mathfrak{A}$ fällt. Werden diese allgemein mit μ, ferner die Wurzeln, zu denen die eigentlichen Darstellungen der Zahl m und ihrer Teiler μ gehören, mit n, bzw. ν bezeichnet, so läßt sich das System f der reduzierten Formen von $\mathfrak{A}$ durch das nachstehende g ersetzen:

$$\begin{array}{llll} (m, \pm n_1, p_1) & (m, \pm n_2, p_2) & (m, \pm n_3, p_3) & \ldots\ldots \\ (\mu_1, \pm \nu_1, \pi_1) & (\mu_2, \pm \nu_2, \pi_2) & (\mu_3, \pm \nu_3, \pi_3) & \ldots\ldots, \end{array}$$

in dem allgemein $p(\pi) = \dfrac{n^2(\nu^2) + \Delta}{m(\mu)}$ gesetzt ist und in dem offenbar mehrere Formen in eine und dieselbe Klasse fallen können. Sämtlichen Formen aus g steht die Beteiligung an der Darstellung von M offen; diese muß, falls DRM, mindestens durch eine unter ihnen erfolgen. Multipliziert man eine beliebige Darstellung von M mit m, bzw. μ:

$$m(\mu)x^2 \pm 2n(\nu)xy + p(\pi)y^2 = M;\ m^2(\mu^2)x^2 \pm 2mn(\mu\nu)xy + n(\nu)y^2 + \begin{pmatrix} mp - n^2 \\ \mu\pi - \nu^2 \end{pmatrix} y^2 = m(\mu)M;\ \begin{pmatrix} mx \pm ny \\ \mu x \pm \nu y \end{pmatrix}^2 + \Delta y^2 = m(\mu)M$$

oder, X für $\begin{matrix} mx \pm ny \\ \mu x \pm \nu y \end{matrix}$, Y für y substituiert:

$$(1) X^2 + \Delta Y^2 = m(\mu)M,$$

so ergibt sich daraus eine Darstellung von mM, bzw. μM durch die Hauptform (1, o, Δ), welche im zweiten Falle nach weiterer Multiplikation mit dem quadratischen Faktor $\frac{m}{\mu}$ ebenfalls in eine der ersteren gleichartige Darstellung übergeht:

$$(1_o) X^2 \cdot \frac{m}{\mu} + \Delta Y^2 \cdot \frac{m}{\mu} = m \cdot M = X_o^2 + \Delta Y_o^2$$

Mit jeder Darstellung von M durch $\mathfrak{A}$ ist also eine solche von $m \cdot M$ durch (1, o, Δ) verbunden. Haben m und seine Teiler μ mit den zugehörigen Wurzeln durchweg den Faktor δ gemein, so geht dieser auch in $X = \frac{mx + ny}{\mu x + \nu y}$ und in $\Delta = \frac{mp - n^2}{\mu\pi - \nu^2}$ auf. Dividiert man Gl. (1) und (1_o) durch δ, so kommt unter Einführung von $X(X_o) = \delta \cdot X'$, $Y(Y_o) = Y'$ und $m = \delta \cdot m'$:

$$(2)\ \delta \cdot X'^2 + \frac{\Delta}{\delta} Y'^2 = m' \cdot M.$$

Die Form $\left(\delta, o, \frac{\Delta}{\delta}\right)$ liefert somit ebenso viele Darstellungen von $m' \cdot M$ als die Hauptform (1, o, Δ) von m . M. Setzt man für die Folge m prim zu M fest und faßt man ferner die 4 Darstellungen, welche sich nur durch die Vorzeichen ihrer Unbestimmten unterscheiden und welche, falls sie eigentlich sind, zu einem Paar entgegengesetzter Wurzeln gehören, zu einer Zerlegung (vgl. S. 19) zusammen, so leitet man unter Beziehung auf die Form $\left(\delta, o, \frac{\Delta}{\delta}\right)$, in der der Fall $\delta = 1$ miteinbegriffen ist, folgende Sätze her:

α) 2 verschiedenen Zerlegungen von M durch $\mathfrak{A}$ entsprechen 2 ebensolche von $m' \cdot M$ durch $\left(\delta, o, \frac{\Delta}{\delta}\right)$. Denn gingen aus den beiden Zerlegungen:

$$M = \mu_1 x_1^2 + 2\nu_1 x_1 y_1 + \pi_1 y_1^2 = \mu_2 x_2^2 + 2\nu_2 x_2 y_2 + \pi_2 y_2^2$$

nur die eine:

$$m'M = \delta X'^2 + \frac{\Delta}{\delta} Y'^2$$

hervor, so würde daraus folgen

$$\left(\frac{m}{\mu_1} = q_1^2,\ \frac{m}{\mu_2} = q_2^2\right).$$

$$Y' = q_1 y_1 = q_2 y_2;\quad X' = q_1\mu'_1 x_1 + q_1\nu'_1 y_1 = q_2\mu'_2 x_2 + q_2\nu'_2 y_2,$$
$$\text{oder } q_1 y_1 = q_2 y_2;\qquad q_1\mu_1 x_1 - q_2\mu_2 x_2 = (\nu_2 - \nu_1)\, q_1 y_1.$$

Die erste Gleichung verlangt, daß q_1 das Produkt $q_2 \cdot y_2$; die zweite, daß q_1 das andere $q_2\mu_2 x_2$ teilt. Hätte nun q_1 mit y_2 und folglich auch mit $\mu_2 \cdot x_2$ einen Faktor gemein, so würde dieser auch in M aufgehn, wodurch m und M in Teilergemeinschaft geräten, was obiger Festsetzung zuwiderläuft. Da mithin q_1 in q_2, umgekehrt aber auch, wie die Einführung von $q_2 y_2$ an Stelle von $q_1 y_1$ in die zweite Gleichung zeigt, q_2 in q_1 enthalten ist, müssen beide und damit ebenfalls μ_1 und μ_2 ($\mu_1 = \mu_2 = \mu$), y_1 und y_2 ($y_1 = y_2 = y$) einander gleich sein. Dadurch geht die zweite Gleichung über in: $\mu(x_1 - x_2) = (\nu_2 - \nu_1) y$. Da ein gemeinschaftlicher Faktor von μ und y auch in M aufginge, M aber zu m und folglich auch zu μ prim ist, muß μ in der Differenz $\nu_2 - \nu_1$ enthalten, somit $\nu_2 \equiv \nu_1 \pmod{\mu}$ oder die Form (μ, ν_2, π_2) dieser (μ, ν_1, π_1) äquivalent sein.

β) Jeder Zerlegung von $m' \cdot M$ durch $\left(\delta, o, \frac{\Delta}{\delta}\right)$ entspricht eine solche von M durch $\mathfrak{A}$. Ist die gegebene Zerlegung

$$(2)\quad \delta \cdot X'^2 + \frac{\Delta}{\delta} Y'^2 = m' \cdot M$$

zunächst uneigentlich, so geht sie nach Beseitigung des größten gemeinsamen Teilers zwischen X'^2 und Y'^2 über in eine eigentliche von $\mu' \cdot M'$, welche mit einer Wurzel N der Kongruenz $x^2 \equiv D \pmod{\mu' \cdot M'}$ verbunden ist. Nach dem Dirichlet'schen Satze über die Zusammensetzung quadratischer Formen (s. seine akademische Gelegenheitsschrift) setzt sich die Klasse, die μ' zur Wurzel N (mod. μ') gehörig darstellt, mit derjenigen aus $\mathfrak{A}$, die M' zur Wurzel N (mod. M') gehörig darstellt, zu einer Klasse zusammen, welche $\mu' \cdot M'$ zur Wurzel N (mod. $\mu' \cdot M'$) gehörig zur Darstellung bringt, welche also mit derjenigen ambigen Klasse zusammenfallen muß, die durch $\left(\delta, o, \frac{\Delta}{\delta}\right)$ vertreten wird. Somit ist der Zerlegung (2) eine eigentliche von M' zugewiesen, welche durch teilweise Hinzunahme des vorhin

entfernten quadratischen Faktors eine uneigentliche Zerlegung von M gibt. Man erkennt:

Die aus (2) abgeleitete Zerlegung ist eigentlich oder uneigentlich, je nachdem es (2) bezüglich M ist.

Entfallen des weiteren auf eine Wurzel N′ von $x^2 \equiv D \pmod{M'}$ 2 Zerlegungen von $m' \cdot M$, so gehen daraus 2 Zerlegungen von M durch äquivalente Formen von $\mathfrak{A}$ hervor, die selbst als uneigentliche nicht auseinander gehalten werden. Weichen aber die beiden Zerlegungen in der Wurzel N′ voneinander ab, so leiten sie auf 2 Zerlegungen von M durch 2 verschiedene Klassen von $\mathfrak{A}$ hin. Somit erhellt die Umkehrung des vorigen Satzes:

2 bezüglich M verschiedene Zerlegungen von m′M durch $\left(\delta, o, \frac{\Delta}{\delta}\right)$ paaren sich mit 2 ebensolchen von M durch $\mathfrak{A}$.

γ) Die Mindestzahl z_{Min} aller Zerlegungen von m′M durch $\left(\delta, o, \frac{\Delta}{\delta}\right)$ ist gleich derjenigen der Zerlegungen von M durch $\mathfrak{A}$; ihre Höchstzahl z_{Max} gleich dem Produkte aus der vorletzt genannten Zahl und derjenigen aller Zerlegungen von m durch $\mathfrak{A}$.

Bedingung für z_{Min} ist, daß m (μ) durch jedes Paar entgegengesetzter Klassen von $\mathfrak{A}$, das an der Zerlegung von M teilnimmt, nur einmal zerlegt wird. Erfolgt dieses durch jenes zur Wurzel n (ν) (mod. m (μ)), eine eigentliche Zerlegung von M (M′) zur Wurzel N (N′) (mod. M (M′)), so setzen sich beide Zerlegungen zu einer eigentlichen von $\frac{m}{(\mu)} \cdot M(M')$ zusammen, welche zu der aus n (ν) und N (N′) vereinigten Wurzel gehört und somit eindeutig bestimmt ist. Sie führt durch eine vielleicht mögliche Division durch δ und durch Wiederaufnahme vielleicht vorher entfernter Quadrate in eine eigentliche (uneigentliche) Zerlegung von mM, bzw. $m' \cdot M$ über. Bedingung für z_{Max} ist, daß $\mathfrak{A}$ einklassig ist oder D zu den $65D_1$ gehört. Jede Zerlegung von m (μ) setzt sich dann mit einer solchen von M (M′) zu einer weiteren von $\frac{m}{(\mu)} \cdot M(M')$ zusammen. Da nun nach dem ersten Satze alle diese zusammen-

gesetzten Zerlegungen in jedem Falle voneinander verschieden sein müssen, es mithin nicht weniger Zerlegungen von $m' \cdot M$ durch $\left(\delta, o \frac{\Delta}{\delta}\right)$; nach dem zweiten Satze aber auch nicht mehr geben kann, folgt, daß für alle Fälle der Gesamtmenge dieser eine gleich große jener gegenübersteht, und damit die Richtigkeit der Behauptung für die besonderen Fälle.

δ) Anwendungen der vorhergehenden Sätze.

Aus dem Totalcharakter, den die zu untersuchende Zahl bzgl. D angibt, bestimmt man zunächst das eigentlich primitive Geschlecht $\mathfrak{A}$ von D, das allein zur Darstellung von M befähigt ist; hierauf die zu $\mathfrak{A}$ gehörende Zahl m gleichzeitig mit den Wurzeln, die ihren oder ihrer Teiler μ Darstellungen durch $\mathfrak{A}$ entsprechen. Hierauf sucht man unter Zugrundelegung der Gauß'schen Ausschließungsmethode die Zerlegungen von $m' \cdot M$ durch $\left(\delta, o, \frac{\Delta}{\delta}\right)$, deren sich nach dem letzten Satze mindestens soviele einstellen müssen, als solche von M durch $\mathfrak{A}$ stattfinden. Schließt man zunächst bzgl. M uneigentliche Zerlegungen aus, so folgert man:

a) Erschließt sich nur eine eigentliche Zerlegung von $m' \cdot M$, so offenbart sich dadurch M als prim.

b) Ergeben sich deren mehrere, so wird M nur dann prim sein, falls sämtliche Wurzeln, zu welchen jene gehören, einander (mod. M) kongruent, M mithin nur durch ein Paar entgegengesetzter Klassen von $\mathfrak{A}$ zu einem Paar entgegengesetzter Wurzeln gehörig, μ dagegen durch jenes mit mehreren dieser verbunden dargestellt wird.

Erweisen sich dagegen zwei oder mehrere jener Wurzeln als (mod. M) inkongruent, so muß M zusammengesetzt sein. Wird m (μ) durch jede Klasse von $\mathfrak{A}$ nur zu einer Wurzel n (ν) gehörig dargestellt, so werden sämtliche Wurzeln der Kongruenz $x^2 \equiv D$ (mod. m'M) einander (mod. M) inkongruent sein. Unter Voraussetzung einer derartigen Hülfszahl m geht ein zusammengesetztes M schon aus 2 Zerlegungen von $\mu' \cdot M$ hervor.

Haben neben den bzgl. M eigentlichen auch die ausgeschlossenen Zerlegungen statt, so fließen aus diesen quadratische Faktoren von M.

Tritt dagegen überhaupt keine Zerlegung von $m' \cdot M$ auf, so ist D Nichtrest einer geraden Anzahl Primteiler von M, M also auf jeden Fall zusammengesetzt. Man verfährt dann nach S. 93.

Aus den eigentlichen Zerlegungen von $\mu' \cdot M$ gehen die Faktoren von M auf zweifachem Wege hervor.

1. Man wendet die Methode von S. 22 darauf an. Wenn M zusammengesetzt ist, was die obige Voraussetzung über die Darstellungsverteilung von m in $\mathfrak{A}$ sicherstellt, so wird jene die Faktoren von M liefern. Gibt sie dagegen nur die bekannte Zerlegung $\mu \cdot M$, so wird man auf ein primes M schließen.

2. Man nimmt die Gaußsche Faktorenbestimmung zur Hülfe. Die Wurzeln der Kongruenz: $x^2 \equiv D \pmod{\mu \cdot M}$ sind denen der andern: $x^2 \equiv D \pmod{M}$ nach dem Modul M kongruent. Summen und Differenzen derselben enthalten die Teiler von M (vgl. S. 91). —

Eine einzige Formuntersuchung leistet also denselben Dienst wie diejenige des vollständigen Formensystems f, die auch Seelhoff nicht beseitigt hat. Allerdings erstreckt sich jene nicht auf die Zahl M selbst, sondern auf ihr m'-faches, deshalb verdienen möglichst kleine m' vor allen anderen den Vorzug. Der Gebrauch der Form $\left(\delta,\ o,\ \frac{\Delta}{\delta}\right)$, $(\delta > 1)$, gewährt einen dreifachen Vorteil. Erstlich ist die zu untersuchende Zahl kleiner, zweitens bleibt i. A. die Wurzelzahl der Kongruenz: $x^2 \equiv y \left(\mathrm{mod.}\ \frac{\Delta}{\delta}\right)$, wo $\delta y \equiv m'M \left(\mathrm{mod.}\ \frac{\Delta}{\delta}\right)$, hinter derjenigen der Kongruenz: $x^2 \equiv m \cdot M \pmod{\Delta}$ zurück, wobei freilich der Modul auch auf seinen δ-Teil zurückgeht, und drittens erniedrigt sich der Bereich der Wurzeln (vgl. D. A. Art. 323).

Einrichtung der Tafel II.

Die Tafel II gibt vor allem Hülfszahlen m für Determinanten im Bereiche von — 1 bis — 207 480, deren eigentlich primitive Geschlechter eine bis vier Klassen umfassen. Sie enthält zunächst die $65 D_1$; sodann ge-

eignete Determinanten der Gaußschen Tafel (vgl. Gauß' Werke Bd. II S. 450), die die negativen Determinanten der 3 ersten Tausende und des 10. Tausend vollständig, vom 5., 6., 7. und 12. Tausend, bzw. das 3., 1., die 3 ersten und die vier letzten Hunderte klassifiziert; schließlich nimmt sie einige wenige Determinanten — darunter deren absolut größte, — 19 320, der Seelhoffschen Tafel auf. Alle übrigen, insbesondere diejenigen außerhalb des Gaußschen Bereiches außer der ebengenannten, hat der Verfasser dieser Arbeit selber hinzugefügt. Da ambige Geschlechter zu große m erfordern, sind mit Ausnahme derjenigen der $65D_1$ der Tafel nur nichtambige oder gemischte Geschlechter $\mathfrak{A}$ eingereiht worden. In dieser Hinsicht stellt Tafel II die Ergänzung der Seelhoffschen dar. Von sämtlichen m′ können nur diese 4, 20, 28, 44, 52 uneigentlich zerlegt werden. Da es übrigens mit Ausnahme der 4 für die 17 Pepinschen Determinanten, dagegen im Verein mit $m' = 2$ der $65D_1$ die einzigen sind, auf die sich zuerst ermittelte Werte m reduzieren, so gilt für die übrigen die Vereinfachung: $\mathbf{m = m' = \mu = \mu'}$. Da ferner alle zusammen durch jedes Paar entgegengesetzter Klassen von $\mathfrak{A}$ nur einmalig zerlegt werden, so stellen in jedem Falle 2 bezgl. M eigentliche Zerlegungen ein zusammengesetztes M fest. Die Determinanten D_3 und D_4 der Tafel verlangen offenbar zusammengesetzte m. In die erste Vertikalspalte sind die Hülfszahlen m in steigender Reihe eingeordnet; in die zweite die dazu gehörigen Determinanten nebst den reduzierten Formen ihrer Geschlechter $\mathfrak{A}$. Diese werden sich mithin soviel Mal wiederholen, als sie Werte m lieferten. Die dritte Vertikalspalte enthält die Totalcharaktere der Geschlechter $\mathfrak{A}$. Da sich die Tafeldeterminanten im großen und ganzen aus den kleinsten Primteilern zusammensetzen, ist jedem derselben bis zu $p = 29$ eine besondere Unterspalte eingeräumt, die zur Aufnahme des auf ihn bezogenen Spezialcharakters dient. Ein + bedeutet den Spezialcharakter Rest, ein — den entgegengesetzten: Nichtrest. Die vorletzte Unterspalte führt den Spezialcharakter bezüglich 4 oder 8, und die letzte steht für einen etwa vorkommenden höhern Primteiler von D offen. Sie gibt den ihm entsprechenden Spezialcharakter in der Gaußschen Bezeichnungsweise an. Die letzte Vertikalspalte schließlich nimmt die Wurzeln der Kongruenz $x^2 \equiv D \pmod{m\,(\mu)}$ auf. Für jedes m entfallen nämlich sämtliche Wurzeln jener Kongruenz auf $\mathfrak{A}$.

Tafel II.

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D\left(\frac{m}{u}\right)$
		3	5	7	11	13	17	19	23	29	4,8		
1	D = — 1 (1, 0, 1)												
"	2 (1, 0, 2)												
"	3 (1, 0, 3)	+											
"	4 (1, 0, 4)										1,4		
"	5 (1, 0, 5)		+								1,4		
"	6 (1, 0, 6)	+									1 u. 7, 8		
"	6 (2, 0, 3)	—									3 u. 5, 8		
"	7 (1, 0, 7)			+									
"	8 (1, 0, 8)										1,8		
"	9 (1, 0, 9)	+									1,4		
"	10 (1, 0, 10)		+								1 u. 3, 8		
"	10 (2, 0, 5)		—								5 u. 7, 8		
"	12 (1, 0, 12)	+									1,4		
"	12 (3, 0, 4)	+									3,4		
"	13 (1, 0, 13)					+					1,4		
"	15 (1, 0, 15)	+	+										
"	15 (3, 0, 5)	—	—										
"	16 (1, 0, 16)										1,8		
"	18 (1, 0, 18)	+									1 u. 3, 8		
"	18 (2, 0, 9)		—								1 u. 3, 8		

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \pmod{m \atop u}$
		3	5	7	11	13	17	19	23	29	4,8		
1	21 (1, 0, 21)	+		+							1,4		
,,	21 (3, 0, 7)	+		−							3,4		
,,	22 (1, 0, 22)				+						1 u. 7, 8		
,,	22 (2, 0, 11)				−						3 u. 5, 8		
,,	24 (1, 0, 24)	+									1,8		
,,	24 (3, 0, 8)	−									3,8		
,,	25 (1, 0, 25)		+								1,4		
,,	28 (1, 0. 28)			+							1,4		
,,	28 (4, 0, 7)			+							3,4		
,,	30 (1, 0, 30)	+	+								1 u. 7, 8		
,,	30 (2, 0, 15)	−	−								1 u. 7, 8		
,,	30 (3, 0, 10)	+	−								3 u. 5, 8		
,,	30 (5, 0, 6)	−	+								3 u. 5, 8		
,,	33 (1, 0, 33)	+			+						1,4		
,,	33 (3, 0, 11)	−			+						3,4		
,,	37 (1, 0, 37)										1,4	R 37	
,,	40 (1, 0, 40)		+								1,8		
,,	40 (5, 0, 8)		−								5,8		
,,	42 (1, 0, 42)	+		+							1 u. 3, 8		
,,	42 (2, 0, 21)	−		+							5 u. 7, 8		

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \pmod{m/u}$
		3	5	7	11	13	17	19	23	29	4,8		
1	42 (3, 0, 14)	−		−							1 u. 3, 8		
”	42 (6, 0, 7)	+		−							5 u. 7, 8		
”	45 (1, 0, 45)	+	+								1,4		
”	45 (5, 0, 9)	−	+								1,4		
”	48 (1, 0, 48)	+									1,8		
”	48 (3, 0, 16)	+									3,8		
”	57 (1, 0, 57)	+						+			1,4		
”	57 (3, 0, 19)	+						−			3,4		
”	58 (1, 0, 58)									+	1 u. 3, 8		
”	58 (2, 0, 29)									−	5 u. 7, 8		
”	60 (1, 0, 60)	+	+								1,4		
”	60 (3, 0, 20)	−	−								3,4		
”	60 (4, 0, 15)	+	+								3,4		
”	60 (5, 0, 12)	−	−								1,4		
”	70 (1, 0, 70)		+	+							1 u. 7, 8		
”	70 (2, 0, 35)		−	+							3 u. 5, 8		
”	70 (5, 0, 14)		+	−							3 u. 5, 8		
”	70 (7, 0, 10)		−	−							1 u. 7, 8		
”	72 (1, 0, 72)	+									1,8		
”	72 (8, 0, 9)										1,8		

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8	
1	78 (1, 0, 78)	+				+					1 u. 7, 8	
"	78 (2, 0, 39)	−				−					1 u. 7, 8	
"	78 (3, 0, 26)	−				+					3 u. 5, 8	
"	78 (6, 0, 13)	+				−					3 u. 5, 8	
"	85 (1, 0, 85)		+				+				1,4	
"	85 (5, 0, 17)		−				−				1,4	
"	88 (1, 0, 88)				+						1,8	
"	88 (8, 0, 11)				−						3,8	
"	93 (1, 0, 93)	+									1,4	R 31
"	93 (3, 0, 31)	+									3,4	N 31
"	102 (1, 0, 102)	+					+				1 u. 7, 8	
"	102 (3, 0, 34)	+					−				3 u. 5, 8	
"	102 (6, 0, 17)	−					−				1 u. 7, 8	
"	102 (2, 0, 51)	−					+				3 u. 5, 8	
"	105 (1, 0, 105)	+	+	+							1,4	
"	105 (3, 0, 35)	−	−	−							3,4	
"	105 (5, 0, 21)	−	+	−							1,4	
"	105 (7, 0, 15)	+	−	+							3,4	
"	112 (1, 0, 112)			+							1,8	
"	112 (7, 0, 16)			+							7,8	

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8		
1	120 (1, 0, 120)	+	+								1,8		
”	120 (3, 0, 40)	+	−								3,8		
”	120 (5, 0, 24)	−	+								5,8		
”	120 (8, 0, 15)	−	−								7,8		
”	130 (1, 0, 130)		+			+					1 u. 3, 8		
”	130 (2, 0, 65)		−			−					1 u. 3, 8		
”	133 (1, 0, 133)			+				+			1,4		
”	133 (7, 0. 19)			−				+			3,4		
”	165 (1, 0, 165)	+	+		+						1,4		
”	165 (3, 0, 55)	+	−		+						3,4		
”	165 (5, 0, 33)	−	+		−						1,4		
”	165 (11, 0, 15)	−	+		+						3,4		
”	168 (1, 0, 168)	+		+							1,8		
”	168 (3, 0, 56)	−		−							3,8		
”	168 (7, 0, 24)	+		−							7,8		
”	168 (8, 0, 21)	−		+							5,8		
”	177 (1, 0, 177)	+									1,4	R 59	
”	177 (3, 0, 59)	−									3,4	R 59	
”	190 (1, 0, 190)		+					+			1 u. 7, 8		
”	190 (2, 0, 95)		−					−			1 u. 7, 8		

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \left(\frac{m}{u}\right)$
		3	5	7	11	13	17	19	23	29	4,8	
1	190 (5, 0, 38)		−					+			3 u. 5, 8	
"	190 (10, 0, 19)		+					−			3 u. 5, 8	
"	210 (1, 0, 210)	+	+	+							1 u. 3, 8	
"	210 (2, 0, 105)	−	−	+							1 u. 3, 8	
"	210 (3, 0, 70)	+	−	−							1 u. 3, 8	
"	210 (5, 0, 42)	−	−	−							5 u. 7, 8	
"	210 (6, 0, 35)	−	+	−							1 u. 3, 8	
"	210 (7, 0, 30)	+	−	+							5 u. 7, 8	
"	210 (10, 0, 21)	+	+	−							5 u. 7, 8	
"	210 (14, 0, 15)	−	+	+							5 u. 7, 8	
"	232 (1, 0, 232)									+	1,8	
"	232 (8, 0, 29)									−	5,8	
"	240 (1, 0, 240)	+	+								1,8	
"	240 (3, 0, 80)	−	−								3,8	
"	240 (5, 0, 48)	−	−								5,8	
"	240 (15, 0, 16)	+	+								7,8	
"	253 (1, 0, 253)				+				+		1,4	
"	253 (11, 0, 23)				+				−		3,4	
"	273 (1, 0, 273)	+		+		+					1,4	
"	273 (3, 0, 91)	+		−		+					3,4	

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{m}$
		3	5	7	11	13	17	19	23	29	4,8	
1	273 (7, 0, 39)	+		+		−					3,4	
"	273 (13, 0, 21)	+		−		−					1,4	
"	280 (1, 0, 280)		+	+							1,8	
"	280 (5, 0, 56)		+	−							5,8	
"	280 (7, 0, 40)		−	−							7,8	
"	280 (8, 0, 35)		−	+							3,8	
"	312 (1, 0, 312)	+				+					1,8	
"	312 (3, 0, 104)	−				+					3,8	
"	312 (13, 0, 24)	+				−					5,8	
"	312 (8, 0, 39)	−				−					7.8	
"	330 (1, 0, 330)	+	+		+						1 u. 3, 8	
"	330 (2, 0, 165)	−	−		−						5 u. 7, 8	
"	330 (3, 0, 110)	−	−		+						1 u. 3, 8	
"	330 (5, 0, 66)	−	+		+						5 u. 7, 8	
"	330 (6, 0, 55)	+	+		−						5 u. 7, 8	
"	330 (10, 0, 33)	+	−		−						1 u. 3, 8	
"	330 (11, 0, 30)	−	+		−						1 u. 3, 8	
"	330 (15, 0, 22)	+	−		+						5 u. 7, 8	
"	345 (1, 0, 345)	+	+						+		1,4	
"	345 (3, 0, 115)	+	−						+		3,4	

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8	
1	345 (5, 0, 69)	−	+						−		1,4	
,,	345 (15, 0, 23)	−	−						−		3,4	
,,	357 (1, 0, 357)	+		+			+				1,4	
,,	357 (3, 0, 119)	−		−			−				3,4	
,,	357 (7, 0, 51)	+		+			−				3,4	
,,	357 (17, 0, 21)	−		−			+				1,4	
,,	385 (1, 0, 385)		+	+	+						1,4	
,,	385 (5, 0, 77)		−	−	+						1,4	
,,	385 (7, 0, 55)		−	−	−						3,4	
,,	385 (11, 0, 35)		+	+	−						3,4	
,,	408 (1, 0, 408)	+					+				1,8	
,,	408 (3, 0, 136)	+					−				3,8	
,,	408 (8, 0, 51)	−					+				3,8	
,,	408 (17, 0, 24)	−					−				1,8	
,,	462 (1, 0, 462)	+		+	+						1 u. 7, 8	
,,	462 (2, 0, 231)	−		+	−						1 u. 7, 8	
,,	462 (3, 0, 154)	+		−	+						3 u. 5, 8	
,,	462 (6, 0, 77)	−		−	−						3 u. 5, 8	
,,	462 (7, 0, 66)	+		−	−						1 u. 7, 8	
,,	462 (11, 0, 42)	−		+	+						3 u. 5, 8	

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8	
1	462 (14, 0, 33)	−		−	+						1 u. 7, 8	
„	462 (21, 0, 22)	+		+	−						3 u. 5, 8	
„	520 (1, 0, 520)		+			+					1,8	
„	520 (5, 0, 104)		+			−					5,8	
„	520 (8, 0, 65)		−			−					1,8	
„	520 (13, 0, 40)		−			+					5,8	
„	760 (1, 0, 760)		+					+			1,8	
„	760 (5, 0, 152)		−					+			5,8	
„	760 (8, 0, 95)		−					−			7,8	
„	760 (19, 0, 40)		+					−			3,8	
„	840 (1, 0, 840)	+	+	+							1,8	
„	840 (3, 0, 280)	+	−	−							3,8	
„	840 (5, 0, 168)	−	−	−							5,8	
„	840 (7, 0, 120)	+	−	+							7,8	
„	840 (8, 0, 105)	−	−	+							1,8	
„	840 (15, 0, 56)	−	+	+							7,8	
„	840 (21, 0, 40)	+	+	−							5,8	
„	840 (24, 0, 35)	−	+	−							3,8	
„	1320 (1, 0, 1320)	+	+		+						1,8	
„	1320 (3, 0, 440)	−	−		+						3,8	

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{m}$
		3	5	7	11	13	17	19	23	29	4,8	
1	1320 (5, 0, 264)	−	+		+						5,8	
,,	1320 (8, 0, 165)	−	−		−						5,8	
,,	1320 (11, 0, 120)	−	+		−						3,8	
,,	1320 (15, 0, 88)	+	−		+						7,8	
,,	1320 (24, 0, 55)	+	+		−						7,8	
,,	1320 (33, 0, 40)	+	−		−						1,8	
,,	1365 (1, 0, 1365)	+	+	+		+					1,4	
,,	1365 (3, 0, 455)	−	−	−		+					3,4	
,,	1365 (5, 0, 273)	−	−	−		−					1,4	
,,	1365 (7, 0, 195)	+	−	−		−					3,4	
,,	1365 (13, 0, 105)	+	−	−		+					1,4	
,,	1365 (15, 0, 91)	+	+	+		−					3,4	
,,	1365 (21, 0, 65)	−	+	+		−					1,4	
,,	1365 (35, 0, 39)	−	+	+		+					3,4	
,,	1848 (1, 0, 1848)	+		+	+						1,8	
,,	1848 (3, 0, 616)	+		−	+						3,8	
,,	1848 (7, 0, 264)	+		−	−						7,8	
,,	1848 (8, 0, 231)	−		+	−						7,8	
,,	1848 (11, 0, 168)	−		+	+						3,8	
,,	1848 (21, 0, 88)	+		+	−						5,8	

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8		
1	1848 (24, 0, 77)	−		−	−						5,8		
”	1848 (33, 0, 56)	−		−	+						1,8		
2	5 (2, 1, 3)		−								3,4		1
”	9 (2, 1, 5)	−									1,4		1
”	13 (2, 1, 7)					−					3,4		1
”	16 (4, 2, 5)										5,8		2
”	21 (2, 1, 11)	−		+							3,4		1
”	24 (4, 2, 7)	+									7,8		2
”	25 (2, 1, 13)		−								1,4		1
”	33 (2, 1, 17)	−			−						1,4		1
”	33 (6, 3, 7)	+			−						3,4		3
”	37 (2, 1, 19)										3,4	N 37	1
”	40 (4, 2, 11)		+								3,8		2
”	45 (2, 1, 23)	−	−								3,4		1
”	48 (4, 2, 13)	+									5,8		2
”	57 (2, 1, 29)	−						−			1,4		1
”	57 (6, 3, 11)	−						+			3,4		3
”	72 (8, 4, 11)	−									3,8		4
”	(4, 2, 19)	+									3,8		2
”	85 (2, 1, 43)		−				+				3,4		1

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \pmod{m/u}$
		3	5	7	11	13	17	19	23	29	4,8		
2	85 (10, 5, 11)		+				−				3,4		5
”	88 (4, 2, 23)				+						7,8		2
”	88 (8, 4, 13)				−						5,8		4
”	93 (2, 1, 47)	−									3,4	R 31	1
”	93 (6, 3, 17)	−									1,4	N 31	3
”	105 (2, 1, 53)	−	−	+							1,4		1
”	105 (6, 3, 19)	+	+	−							3,4		3
”	105 (10, 5, 13)	+	−	−							1,4		5
”	112 (4, 2, 29)			+							5,8		2
”	120 (4, 2, 31)	+	+								7,8		2
”	120 (8, 4, 17)	−	−								1,8		4
”	120 (12, 6, 13)	+	−								5,8		6
”	133 (2, 1, 67)			+				−			3,4		1
”	165 (2, 1, 83)	−	−		−						3,4		1
”	165 (6, 3, 29)	−	+		−						1,4		3
”	165 (10, 5, 19)	+	+		−						3,4		5
”	168 (4, 2, 43)	+		+							3,8		2
”	168 (8, 4, 23)	−		+							7,8		4
”	168 (12, 6, 17)	−		−							1,8		6
”	177 (2, 1, 89)	−									1,4	N 59	1

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8		
2	177 (6, 3, 31)	+									3,4	N 59	3
"	232 (4, 2, 59)									+	3,8		2
"	232 (8, 4, 31)									−	7,8		4
"	240 (4, 2, 61)	+	+								5,8		2
"	240 (12, 6, 23)	−	−								7,8		6
"	240 (16, 8, 19)	+	+								3,8		8
"	253 (2, 1, 127)				−				+		3,4		1
"	273 (2, 1, 137)	−		+		−					1,4		1
"	273 (14, 7, 23)	−		+		+					3,4		7
"	273 (6, 3, 47)	−		−		−					3,4		3
"	280 (4, 2, 71)		+	+							7,8		2
"	280 (8, 4, 37)		−	+							5,8		4
"	312 (4, 2, 79)	+				+					7,8		2
"	312 (8, 4, 41)	−				−					1,8		4
"	312 (12, 6, 29)	−				+					5,8		6
"	345 (2, 1, 173)	−	−						+		1,4		1
"	345 (6, 3, 59)	−	+						+		3,4		3
"	345 (10, 5, 37)	+	−						−		1,4		5
"	357 (2, 1, 179)	−		+			+				3,4		1
"	357 (6, 3, 61)	+		−			−				1,4		3

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8	
2	357 (14, 7, 29)	−		+			−				1,4	7
”	385 (2, 1, 193)		−	+	−						1,4	1
”	385 (10, 5, 41)		+	−	−						1,4	5
”	385 (14, 7, 31)		+	−	+						3,4	7
”	385 (22, 11, 23)		−	+	+						3,4	11
”	408 (4, 2, 103)	+					+				7,8	2
”	408 (8, 4, 53)	−					+				5,8	4
”	408 (12, 6, 37)	+					−				5,8	6
”	520 (4, 2, 131)		+			+					3,8	2
”	520 (8, 4, 67)		−			−					3,8	4
”	520 (20, 10, 31)		+			−					7,8	10
”	760 (4, 2, 191)		+					+			7,8	2
”	760 (8, 4, 97)		−					−			1,8	4
”	760 (20, 10, 43)		−					+			3,8	10
”	840 (4, 2, 211)	+	+	+							3,8	2
”	840 (8, 4, 107)	−	−	+							3,8	4
”	840 (12, 6, 73)	+	−	−							1,8	6
”	840 (20, 10, 47)	−	−	−							7,8	10
”	840 (24, 12, 44)	−	+	−							1,8	12
”	840 (28, 14, 37)	+	−	+							5,8	14

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{m}$
		3	5	7	11	13	17	19	23	29	4,8	
2	1320 (4, 2, 331)	+	+		+						3,8	2
"	1320 (8, 4, 167)	−	−		−						7,8	4
"	1320 (12, 6, 113)	−	−		+						1,8	6
"	1320 (20, 10, 71)	−	+		+						7,8	10
"	1320 (24, 12, 61)	+	+		−						5,8	12
"	1320 (40, 20, 43)	+	−		−						3,8	20
"	1365 (2, 1, 683)	−	−	+		−					3,4	1
"	1365 (6, 3, 229)	+	+	−		−					1,4	3
"	1365 (10, 5, 139)	+	+	−		+					3,4	5
"	1365 (14, 7, 101)	−	+	−		+					1,4	7
"	1365 (26, 13, 59)	−	+	−		−					3,4	13
"	1365 (30, 15, 53)	−	−	+		+					1,4	15
"	1365 (42, 21, 43)	+	−	+		+					3,4	21
"	1848 (4, 2, 463)	+		+	+						7,8	2
"	1848 (8, 4, 233)	−		+	−						1,8	4
"	1848 (12, 6, 157)	+		−	+						5,8	6
"	1848 (24, 12, 83)	−		−	−						3,8	12
"	1848 (28, 14, 73)	+		−	−						1,8	14
"	1848 (44, 22, 53)	−		+	+						5,8	22
3	8 (3, 1, 3)										3,8	± 1

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8	
4	123 (1, 0, 123) (4, ± 1, 31)	+										R 41	0, ± 1
"	163 (1, 0, 163) (4, ± 1, 41)											R 163	0, ± 1
"	187 (1, 0, 187) (4, ± 1, 47)				+		+						0, ± 1
"	195 (1, 0, 195) (4, ± 1, 49)	+	+		+	+							0, ± 1
"	235 (1, 0, 235) (4, ± 1, 59)		+									R 47	0, ± 1
"	267 (1, 0, 267) (4, ± 1, 67)	+										R 89	0, ± 1
"	315 (1, 0, 315) (4, ± 1, 79)	+	+	+									0, ± 1
"	403 (1, 0, 403) (4, ± 1, 101)					+						R 31	0, ± 1
"	427 (1, 0, 427) (4, ± 1, 107)			+								R 61	0, ± 1
"	435 (1, 0, 435) (4, ± 1, 109)	+	+							+			0, ± 1
"	483 (1, 0, 483) (4, ± 1, 121)	+		+					+				0, ± 1
"	532 (8, ± 2, 67)			+				−			3,4		± 2
"	555 (1, 0, 555) (4, ± 1, 139)	+	+									R 37	0, ± 1
"	595 (1, 0, 595) (4, ± 1, 149)		+	+			+						0, ± 1
"	627 (1, 0, 627) (4, ± 1, 157)	+			+			+					0, ± 1
"	715 (1, 0, 715) (4, ± 1, 179)		+		+	+							0, ± 1
"	795 (1, 0, 795) (4, ± 1, 199)	+	+									R 53	0, ± 1
"	1012 (8, ± 2, 127)				−				+		3,4		± 2
"	1092 (8, ± 2, 137)	−		+		−					1,4		± 2
"	1428 (8, ± 2, 179)	−		+			+				3,4		± 2

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8	
4	1435 (1,0,1435)(4,±1,359)		+	+								R 41	0, ± 1
"	5460 (8, ± 2, 683)	−	−	+		−					3,4		± 2
5	21 (5, 2, 5)	−		−							1,4		± 2
"	24 (5, 1, 05)	−									5,8		± 1
"	504 (5, ± 1, 101)	−		−							5,8		± 1
"	561 (5, ± 2, 113)	−			+		−				1,4		± 2
"	609 (5, ± 1, 122)	−		−						+	1,4		± 1
"	616 (5, ± 2, 124)			−	+						5,8		± 2
"	624 (5, ± 1, 125)	−				−					5,8		± 1
7	40 (7, 3, 7)		−								7,8		± 3
"	45 (7, 2, 7)	+	−								3,4		± 2
"	48 (7, 3, 7)	+									7,8		± 3
"	510 (7, ± 1, 73)	+	−				−				1 u. 7, 8		± 1
"	528 (7, ± 2, 76)	+			−						7,8		± 2
"	552 (7, ± 1, 79)	+							−		7,8		± 1
"	570 (7, ± 2, 82)	+	−					+			5 u. 7, 8		± 2
"	598 (7, ± 2, 86)					−			−		1 u. 7, 8		± 2
"	600 (7, ± 3, 87)	+	−								7,8		± 3
"	720 (7, ± 1, 103)	+	−								7,8		± 1
"	880 (7, ± 3, 127)		−		−						7,8		± 3

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8		
7	957 (7, ± 3, 138)	+			−					+	3,4		± 3
"	1032 (7, ± 2, 148)	+									7,8	N 43	± 2
"	1105 (7, ± 1, 158)		−			−	−				3,4		± 1
"	1560 (7, ± 1, 223)	+	−			−					7,8		± 1
"	2040 (7, ± 2, 292)	+	−				−				7,8		± 2
"	2145 (7, ± 2, 307)	+	−		−	−					3,4		± 2
"	2280 (7, ± 3, 327)	+	−					+			7,8		± 3
11	105 (11, 4, 11)	−	+	+							3,4		± 4
"	112 (11, 3, 11)			+							3,8		± 3
"	120 (11, 1, 11)	−	+								3,8		± 1
"	505 (11, ± 1, 46)		+		−						3,4		± 1
"	525 (11, ± 5, 50)	−	+	+							3,4		± 5
"	552 (11, ± 3, 51)	−							−		3,8		± 3
"	568 (11, ± 2, 52)										3,8	N 71	± 2
"	585 (11, ± 3, 54)	−	+			−					3,4		± 3
"	600 (11, ± 4, 56)	−	+								3,8		± 4
"	645 (11, ± 2, 59)	−	+								3,4	R 43	± 2
"	765 (11, ± 4, 83)	−				−			−		3,4		± 4
"	777 (11, ± 2, 71)	−		+							3,4	R 37	± 2
"	798 (11, ± 4, 74)	−		+				+			3 u. 5, 8		± 4

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{m}$
		3	5	7	11	13	17	19	23	29	4,8	
11	805 (11, ± 3, 74)		+	+					−		3,4	± 3
"	897 (11, ± 4, 83)	−				−			−		3,4	± 4
"	910 (11, ± 5, 85)		+	+		−					3 u. 5, 8	± 5
"	912 (11, ± 1, 83)	−						+			3,8	± 1
"	952 (11, ± 4, 88)			+			−				3,8	± 4
"	1008 (11, ± 2, 92)	−		+							3,8	± 2
"	1110 (11, ± 1, 101)	−	+								3 u. 5, 8	R 37 ± 1
"	1128 (11, ± 4, 104)	−									3,8	N 47 ± 4
"	1185 (11, ± 5, 110)	−	+								3,4	R 79 ± 5
"	1240 (11, ± 5, 115)		+								3,8	N 31 ± 5
"	1360 (11, ± 2, 124)		+				−				3,8	± 2
"	2730 (11, ± 3, 249)	−	+	+		−					1 u. 3, 8	± 3
"	2760 (11, ± 1, 251)	−	+						−		3,8	± 1
"	3570 (11, ± 4, 326)	−	+	+			−				1 u. 3, 8	± 4
"	10920 (11, ± 5, 995)	−	+	+		−					3,8	± 5
13	133 (13, 6, 13)			−				−			1,4	± 6
"	165 (13, 2, 13)	+	−		−						1,4	± 2
"	168 (13, 1, 13)	+		−							5,8	± 1
"	660 (13, ± 4, 52)	+	−		−						1,4	± 4
"	672 (13, ± 2, 52)	+		−							5,8	± 2

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8	
13	690 (13, ± 5, 55)	+	−						+		5,8	± 5
”	693 (13, ± 3, 54)	+		−	−						1,4	± 3
”	777 (13, ± 4, 61)	+		−							1,4	N 37 ± 4
”	792 (13, ± 1, 61)	+			−						5,8	± 1
”	805 (13, ± 1, 62)		−	−					+		1,4	± 1
”	870 (13, ± 1, 67)	+	−							+	3 u. 5, 8	± 1
”	1005 (13, ± 3, 78)	+	−								1,4	N 67 ± 3
”	1065 (13, ± 1, 82)	+	−								1,4	N 71 ± 1
”	1122 (13, ± 3, 87)	+			−		+				5 u. 7, 8	± 3
”	1197 (13, ± 5, 94)	+		−				−			1,4	± 5
”	1288 (13, ± 5, 101)			−					+		5,8	± 5
”	1290 (13, ± 6, 102)	+	−								5 u. 7, 8	R 43 ± 6
”	1353 (13, ± 5, 106)	+			−						1,4	N 41 ± 5
”	1785 (13, ± 3, 138)	+	−	−			+				1,4	± 3
”	2040 (13, ± 1, 157)	+	−				+				5,8	± 1
”	2310 (13, ± 2, 178)	+	−	−	−						3 u. 5, 8	± 2
”	2640 (13, ± 5, 205)	+	−	−	−						5,8	± 5
”	3045 (13, ± 6, 237)	+	−	−						+	1,4	± 6
”	3480 (13, ± 2, 268)	+	−							+	5,8	± 2
”	4488 (13, ± 6, 348)	+			−		+				5,8	± 6

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \pmod{m/u}$
		3	5	7	11	13	17	19	23	29	4,8		
13	9240 (13, ± 4, 712)	+	−	−	−						5,8		± 4
17	240 (17, 7, 17)	−	−								1,8		± 7
”	253 (17, 6, 17)				−				−		1,4		± 6
”	273 (17, 4, 17)	−		−		+					1,4		± 4
”	280 (17, 3, 17)		−	−							1,8		± 3
”	528 (17, ± 4, 32)	−			−						1,8		± 4
”	553 (17, ± 5, 34)			−							1,4	N 79	± 5
”	616 (17, ± 8, 40)			−	−						1,8		± 8
”	858 (17, ± 3, 51)	−			−	+					1 u. 7, 8		± 3
”	960 (17, ± 3, 57)	−	−								1,8		± 3
”	1045 (17, ± 3, 62)		−		−			+			1,4		± 3
”	1113 (17, + 3, 66)	−		−							1,4	R 53	± 3
”	1120 (17, ± 6, 68)		−	−							1,8		± 6
”	1488 (17, ± 5, 89)	−									1,8	N 31	± 5
”	1653 (17, ± 8, 101)	−						+		−	1,4		± 8
”	1752 (17, ± 4, 104)	−									1,4	N 73	± 4
”	1885 (17, ± 6, 113)	−				+				−	1,4		± 6
”	3045 (17, ± 7, 182)	−	−	−						−	1,4		± 7
”	4048 (17, ± 7, 241)				−				−		1,8		± 7
”	4305 (17, ± 8, 257)	−	−	−							1,4	N 41	± 8

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8		
17	8008 (17, ± 4, 472)			−	−	+					1,8		± 4
"	19320 (17, ± 3, 1137)	−	−	−					−		1,8		± 3
19	280 (19, 9, 19)		+	−							3,8		± 9
"	312 (19, 7, 19)	+				−					3,8		± 7
"	345 (19, 4, 19)	+	+						−		3,4		± 4
"	357 (19, 2, 19)	+		−		+					3,4		± 2
"	592 (19, ± 4, 32)										3,8	N 37	± 4
"	658 (19, ± 8, 38)			−							1 u. 3, 8	N 47	± 8
"	697 (19, ± 5, 38)						+				3,4	N 41	± 5
"	1248 (19, ± 5, 67)	+				−					3,8		± 5
"	1302 (19, ± 3, 69)	+		−							3 u. 5, 8	R 31	± 3
"	1380 (19, ± 8, 76)	+	+						−		3,4		± 8
"	1428 (19, ± 4, 76)	+		−			+				3,4		± 4
"	1705 (19, ± 9, 94)		+		−						3,4	R 31	± 9
"	1870 (19, ± 7, 101)		+		−		+				3 u. 5, 8		± 7
"	2013 (19, ± 1, 106)	+			−						3,4	R 61	± 1
"	2233 (19, ± 3, 118)			−	−					−	3,4		± 3
"	3480 (19, ± 4, 184)	+	+							−	3,8		± 4
"	5005 (19, ± 7, 266)		+	−	−	−					3,4		± 7
"	5520 (19, ± 3, 291)	+	+						−		3,8		± 3

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \pmod{m/u}$
		3	5	7	11	13	17	19	23	29	4,8		
19	10920 (19, ± 9, 579)	+	+	−		−					3,8		± 9
20	564 (19, ± 5, 31) (15, ± 6, 40)	+									3,4	R 47	± 6, 14
„	1716 (40, ± 2, 43) (40, ± 18, 51)	+			−	+					3,4		± 2, 18
„	2436 (40, ± 2, 61) (40, ± 18, 69)	+		−						−	1,4		± 2, 18
23	408 (23, 11, 23)	−					−				7,8		± 11
„	520 (23, 3, 23)		−			+					7,8		± 3
„	1632 (23, ± 1, 71)	−					−				7,8		± 1
„	1677 (23, ± 5, 74)	−				+					3,4	R 43	± 5
„	1768 (23, ± 7, 79)					+		−			7,8		± 7
„	1992 (23, ± 3, 87)	−									7,8	R 83	± 3
„	2080 (23, ± 6, 92)		−			+					7,8		± 6
„	3465 (23, ± 10, 155)	−	−	+	+						3,4		± 10
„	4680 (23, ± 9, 207)	−	−			+					7,8		± 9
„	6160 (23, ± 2, 268)		−	+	+						7,8		± 2
28	852 (17, ± 7, 53) (21, ± 3, 41)	−									1,4	N 71	± 10, 18
„	1140 (21, ± 6, 56) (29, ± 7, 41)	−	+					−			1,4		± 6, 22
„	1860 (35, ± 10, 56) (39, ± 18, 56)	−	+								3,4	R 31	± 10, 18
29	760 (29, 9, 29)		+					−			5,8		± 9

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8	
29	840 (29, 1, 29)	−	+	+							5,8	± 1
,,	2002 (29, ± 12, 74)			+	−	+					5 u. 7, 8	± 12
,,	2170 (29, ± 11, 79)		+	+							5 u. 7, 8	N 31 ± 11
,,	4305 (29, ± 4, 149)	−	+	+							1,4	N 41 ± 4
,,	4830 (29, ± 10, 170)	−	+	+					+		3 u. 5, 8	± 10
,,	10920 (29, ± 10, 380)	−	+	+		+					5,8	± 10
,,	19320 (29, ± 9, 669)	−	+	+					+		5,8	± 9
31	840 (31, 11, 31)	+	+	−							7,8	± 11
,,	2088 (31, ± 12, 72)	+								−	7,8	± 12
33	560 (17, ± 1, 33) (20, ± 10, 33)		−	−							1,8	± 1, 10
,,	728 (24, ± 8, 33) (28, ± 14, 33)			−		−					1,8	± 8, 14
,,	1520 (33, ± 8, 48) 33, ± 14, 52)		−					−			1,8	± 8, 14
,,	4760 (33, ± 5, 145) (33, ± 16, 152)		−	−			+				1,8	± 5, 16
35	544 (16, ± 4, 35) (19, ± 8, 32)						+				3,8	± 4, 11
,,	696 (20, ± 2, 35) (24, 12, 35)	−								+	3,8	± 2, 12
,,	741 (23, ± 8, 35) (26, 13, 35)	−				+		+			3,4	± 8, 13
,,	936 (27, ± 3, 35) (35, 17, 35)	−				+					3,8	± 3, 17

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8		
35	969 (30, ± 9, 35) (35, 16, 35)	−					+	+			3,4		± 9, 16
„	1144 (35, 9, 35) (35, ± 16, 40)				−	+					3,8		± 9, 16
37	1320 (37, 7, 37)	+	−		+						5,8		± 7
„	1365 (37, 2, 37)	+	−	+		−					1,4		± 2
„	5520 (37, ± 17, 157)	+	−						−		5,8		± 17
„	21840 (37, ± 8, 592)	+	−	+		−					5,8		± 8
39	560 (15, ± 5, 39) (16, 8, 39)		+	+							7,8		± 5, 8
„	680 (20, 10, 39) (24, ± 8, 31)		+				−				7,8		± 8, 10
„	3080 (39, ± 1, 79) (39, ± 25, 95)		+	+	−						7,8		± 1, 25
41	1320 (41, 19, 41)	−	+		−						1,8		± 19
43	1848 (43, 1, 43)	+		+	−						3,8		± 1
„	21840 (43, ± 2, 508)	+	−	+		+					3,8		± 2
44	2340 (27, ± 6, 88) (43, ∓ 5, 55)	+	−			+					3,4		± 6, 38
„	3108 (39, ± 18, 88) (43, ∓ 17, 79)	+		+							3,4	N 37	± 18, 26
„	3220 (37, ± 6, 88) (53, ∓ 15, 65)		−	+					−		1,4		± 6, 38
„	6580 (77, ± 14, 88) (85, ∓ 30, 88)		−	+							1,4	N 47	± 14, 30
47	1848 (47, 19, 47)	−		−	+						7,8		± 19

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8		
51	560 (16, 0, 35) (11, ± 1, 51)		+	+							3,8		± 0, 1
„	665 (14, 7, 51) (15, ± 10, 51)		+	+				−			3,4		± 7, 10
„	1430 (29, ± 7, 51) (30, ± 10, 51)		+		−	+					3 u. 5, 8		± 7, 10
52	4260 (41, ± 2, 104) (65, ± 15, 69)	−	+								1,4	N 71	± 2, 50
„	7140 (69, ± 6, 104) (89, ± 43, 101)	−	+	−			+				1,4		± 6, 46
53	21840 (53, ± 7, 413)	−	−	+		+					5,8		± 7
55	816 (15, ± 3, 55) (16, 8, 55)	+					+				7,8		± 3, 8
„	1176 (24, 12, 55) (31, ± 8, 40)	+		−							7,8		± 12, 23
,	1416 (31, ± 14, 52) (39, ± 12, 40)	+									7,8	N 59	± 17, 27
„	1449 (27, ± 6, 55) (31, ± 15, 54)	+		−					+		3,4		± 6, 16
„	1624 (31, ± 9, 55) (40, ± 16, 47)			−						−	7,8		± 9, 24
„	2184 (40, ± 4, 55) (52, 26, 55)	+		−		+					7,8		± 4, 26
„	2856 (52, ± 4, 55) (55, 13, 55)	+		−			+				7,8		± 2, 13
„	4641 (55, ± 12, 87) (55, ± 23, 94)	+		−		+	+				3,4		± 12, 23
57	1085 (22, ± 13, 57) (30, ± 5, 37)		−	+							1,4	N 31	± 13, 25

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8	
57	1610 (30, ± 10, 57) (42, ± 14, 43)		—	+					—		1 u. 3, 8	$\pm 10, 28$
„	4760 (57, ± 16, 88) (57, ± 22, 92)		—	+			—				1,8	$\pm 16, 22$
„	6440 (57, ± 1, 113) (57, ± 20, 120)		—	+					—		1,8	$\pm 1, 20$
65	1104 (17, ± 1, 65) (20, ± 6, 57)	—							—		1,8	$\pm 1, 14$
„	1221 (21, ± 9, 62) (30, ± 3, 41)	—			—						1,4	R 37 $\pm 12, 27$
„	1309 (22, 11, 65) (29, ± 5, 46)			+	—		—				1,4	$\pm 11, 24$
„	1596 (29, ± 12, 60) (32, ± 10, 53)	—		+				—			1,4	$\pm 17, 22$
„	2584 (40, ± 4, 65) (41, ± 9, 65)						—	—			1,8	$\pm 4, 9$
„	2856 (44, ± 4, 65) (56, 28, 65)	—		+			—				1,8	$\pm 2, 28$
„	3696 (57, ± 3, 65) (65, 23, 65)	—		+	—						1,8	$\pm 3, 23$
„	3864 (60, ± 6, 65) (65, 19, 65)	—		+					—		1,8	$\pm 6, 19$
„	6384 (65, ± 21, 105) (65, ± 31, 113)	—		+				—			1,8	$\pm 21, 31$
77	1020 (17, 0, 60) (32, ± 6, 33)	—	—				+				1,4	$\pm 17, 38$
„	1245 (17, ± 8, 77) (33, ± 3, 38)	—	—								1,4	R 83 $\pm 8, 36$

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8	
77	1272 (24, 0, 77) (29, ± 2, 44)	−									5,8	R 53	± 0, 31
„	1392 (21, ± 6, 68) (29, 0, 48)	−								+	5,8		± 0, 15
„	1608 (21, ± 3, 77) (29, ± 4, 56)	−								+	5,8		± 3, 25
„	1872 (29, ± 10, 68) (36, ± 6, 53)	−				+					5,8		± 19, 30
„	1938 (26, ± 8, 77) (42, ± 6, 47)	−					+	+			5 u. 7, 8		± 8, 36
„	2320 (32, ± 12, 77) (37, ± 14, 68)		−							−	5,8		± 12, 23
„	2397 (33, ± 12, 77) (38, ± 15, 69)	−					+				1,4	N 47	± 12, 54
„	2400 (32, ± 8, 77) (48, ± 12, 53)	+	−								5,8		± 8, 36
„	9880 (77, ± 19, 133) (77, ± 30, 140)		−			+		+			5,8		± 19, 30
85	1254 (19, 0, 66) (30, ± 6, 43)	+			−			+			3 u. 5, 8		± 0, 36
„	1974 (30, ± 6, 67) (43, ± 2, 46)	+		+							3 u. 5, 8	N 47	± 24, 41
„	2184 (28, 14, 85) (37, ± 6, 60)	+		+		−					5;8		± 14, 31
„	2296 (29, ± 13, 85) (44, ± 6, 53)			+							5,8	N 41	± 13, 38
„	2821 (37, ± 18, 85) (46, ± 13, 65)			+		−					1,4	N 31	± 18, 33

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8		
85	5016 (61, ± 13, 85) (76, 38, 85)	+			−			+			5,8		± 13, 38
„	5544 (72, ± 24, 85) (85, 41, 85)	+		+	−						5,8		± 24, 41
„	7161 (85, 8, 85) (85, ± 42, 105)	+		+	−	−					1,4		± 8, 42
87	2072 (24, ± 4, 87) (31, ± 6, 68)			−							7,8	N 37	± 4, 25
91	1200 (16, 0, 75) (19, ± 4, 64)	+	+								3,8		± 0, 23
„	2337 (31, ± 9, 78) (46, ± 3, 51)	+						−			3,4	R 41	± 22, 43
„	2365 (26, ± 1, 91) (34, ± 7, 71)		+		+						3,4	N 43	± 1, 27
„	2805 (31, ± 4, 91) (34, 17, 91)	+	+		+		−				3,4		± 4, 17
„	5032 (56, ± 8, 91) (68, 34, 91)						−				3,8	N 31	± 8, 34
„	6072 (67, ± 5, 91) (88, 44, 91)	+			+				−		3,8		± 5, 44
„	6270 (69, ± 3, 91) (70, ± 10, 91)	+	+		+			−			3 u. 5, 8		± 3, 10
„	8265 (91, 4, 91) (91, ± 17, 94)	+	+					−		+	3,4		± 4, 17
95	2184 (39, 0, 56) (23, ± 1, 95)	−		+		+					7,8		± 0, 1
„	2706 (29, ± 7, 95) (30, ± 12, 95)	−			−						5 u. 7, 8	N 41	± 7, 12

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$										Wurz. der Kongr. $x^2 \equiv D \pmod{\frac{m}{u}}$
		3	5	7	11	13	17	19	23	29	4,8	
95	6006 (65, ± 13, 95) (74, ∓ 32, 95)	−		+	−	+					1 u. 7, 8		± 13, 32
„	6216 (71, ± 23, 95) (84, 42, 95)	−		+							7,8	R 37	± 23, 42
„	24024 (95, ± 26, 260) (95, ∓ 31, 263)	−		+	−	+					7,8		± 26, 31
115	54264 (115, ± 4, 272) (115, ∓ 19, 275)	+		−			+	+			3,8		± 4, 19
119	2112 (23, ± 2, 92) (47, ∓ 12, 48)	−			+						7,8		± 25, 59
„	2665 (31, ± 1, 86) (46, ∓ 7, 59)		+			−					3,4	R 41	± 32, 53
„	4560 (39, ± 9, 119) (44, ∓ 18, 111)	−	+					+			7,8		± 9, 26
„	5640 (56, ± 24, 111) (71, ∓ 18, 84)	−	+								7,8	R 47	± 32, 53
123	2465 (30, ± 5, 83) (38, ∓ 9, 67)		−				+			+	3,4		± 35, 47
133	2397 (22, ± 1, 109) (46, ∓ 15, 57)	+					−				1,4	N 47	± 23, 61
„	4290 (55, 0, 78) (42, ± 6, 103)	+	−		+	+					5 u. 7, 8		± 36, 55
„	5848 (44, ± 2, 133) (56, ∓ 16, 109)						−				5,8	R 43	± 2, 40
„	17160 (133, 23, 133) (133, ± 61, 157)	+	−		+	+					5,8		± 23, 61
143	3990 (36, ± 6, 122) (38, 0, 105)	−	−	−				−			1 u. 7, 8		± 27, 38

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \left(\frac{m}{u}\right)$
		3	5	7	11	13	17	19	23	29	4,8		
143	5565 (42, 21, 143) (47, ± 13, 122)	−	−	−							3,4	R 53	± 21, 34
„	7905 (62, 31, 143) (78, ± 21, 107)	−	−				−				3,4	R 31	± 31, 57
„	15960 (132, ± 54, 143) (143, 67, 143)	−	−	−				−			7,8		± 54, 67
145	5544 (40, ± 16, 145) (73, ± 2, 76)	+		−	−						1,8		± 16, 71
„	54264 (145, ± 16, 376) (145, ± 71, 409)	+		−			+	−			1,8		± 16, 71
161	22440 (140, ± 10, 161) (161, 59, 161)	−	+		−		+				1,8		± 10, 59
177	6545 (37, ± 2, 177) (58, ± 3, 113)		−	+	+		−				1,4		± 2, 61
187	9165 (58, ± 17, 163) (67, ± 9, 138)	+	−			−					3,4	N 47	± 41, 58
„	12040 (68, ± 26, 187) (83, ± 24, 152)		−	−							3,8	N 43	± 26, 59
„	14973 (82, ± 19, 187) (87, ± 36, 187)	+		−					+		3,4	R 31	± 19, 36
„	24360 (132, ± 18, 187) (168, 84, 187)	+	−	−						+	3,8		± 18, 84
209	9765 (54, ± 15, 185) (89, ± 5, 110)	−	+	−							1,4	N 31	± 39, 94
„	11832 (57, ± 9, 209) (92, ± 6, 129)	−					−			+	1,8		± 9, 86
„	11985 (65, ± 25, 194) (74, ± 15, 165)	−	+				−				1,4	R 47	± 40, 59

m (m')	Determinanten und Geschlechter $\mathfrak{A}$	Totalcharakter von $\mathfrak{A}$											Wurz. der Kongr. $x^2 \equiv D \pmod{m/u}$
		3	5	7	11	13	17	19	23	29	4,8		
209	17080 (89, ± 39, 209) (124, ± 30, 145)		+	−							1,8	N 61	± 39, 94
„	26520 (129, ± 21, 209) (156, 78, 209)	−	+			+	−				1,8		± 21, 78
217	57720 (217, ± 39, 273) (217, ± 101, 313)	+	−			+					1,8	N 37	± 39, 101
221	6510 (35. 0, 186) (51, ± 18, 134)	−	+	+							3 u. 5, 8	R 31	± 0, 69
„	26040 (140, 70, 221) (149, ± 84, 221)	−	+	+							5,8	R 31	± 70, 84
„	31080 (141, ± 9, 221) (149, ± 43, 221)	−	+	+							5,8	R 37	± 9, 43
247	28560 (127, ± 53, 247) (172, ± 54, 183)	+	−	+			+				7,8		± 53, 118
„	52360 (212, ± 2, 247) (247, 93, 247)		−	+	+		+				7,8		± 2, 93
323	120120 (323, ± 6, 372) (323, ± 108, 408)	−	−	+	+	−					3,8		± 6, 108
377	157080 (377, ± 135, 465) (377, ± 164, 488)	−	−	−	+		−				1,8		± 135, 164
437	185640 (437, 73, 437) (437, ± 111, 453)	−	−	−		−	−				5,8		± 73, 111
851	207480 (344, ± 52, 611) (371, ± 42, 564)	−	+	+		+		−			3,8		± 292, 329

Die zweite Gaußsche Methode samt ihren Erweiterungen soll auf 4 Beispiele angewandt werden.

1) M = 18518809.

18518809 ist $\equiv 1 \pmod 8$ $\equiv 1 \pmod 3$ $\equiv 1 \pmod 7$ $\equiv 1 \pmod{11}$; mithin Rest von 3, 7 und 11. M kann demnach durch das Hauptgeschlecht G_H der Determinante $D_1 = -1848$ dargestellt werden, was sicherlich eintritt, falls M prim ist. Die repräsentierende Form dieses Geschlechts ist (1, 0, 1848) (vgl. S. 120). Je nachdem M durch (1, 0, 1848) einmalig oder mehrmalig zerlegt wird, ist M prim oder zusammengesetzt. Man sucht also sämtliche Zerlegungen von M durch (1, 0, 1848) oder sämtliche positive Lösungen der Gleichung:

$$x^2 + 1848y^2 = 18\,518\,809.$$

Die notwendige Bedingung für die erste Unbestimmte x ist, daß sie der Kongruenz

$$x^2 \equiv 18\,518\,809 \pmod{1848}$$

genügt; nur Wurzeln dieser Kongruenz sind als Werte x zulässig. Demnach handelt es sich in erster Linie darum, alle jene Wurzeln im Bereiche von x oder den Komplex Ω (vgl. D. A. 323) zu ermitteln, welch' ersterer sich von $x = 0$ bis zu $x = \sqrt{18518809}$ für $y = 0$ erstreckt, dem also als letzte ganze Zahl 4303 angehört ($x \leq 4303$). Die Kongruenz $x^2 \equiv M \pmod{1848}$ besitzt 32 (mod. 1848) inkongruente Wurzeln, welche

$$\equiv \pm 1 \pmod 3 \quad \equiv \pm 1 \pmod 7 \quad \equiv \pm 1 \pmod{11} \text{ und}$$
$$\equiv \pm 1, 3 \pmod 8$$

sind; mithin gehen sie durch Kombination dieser Reste hervor. Ihre positiv kleinsten Werte sind folgende:

1, 43, 155, 197, 265, 307, 419, 461, 463, 505, 617, 659, 727, 769, 881, 923, 925, 967, 1079, 1121, 1189, 1231, 1343, 1385, 1387, 1429, 1541, 1583, 1651, 1693, 1805, 1847.

Nimmt man die ihnen (mod. 1848) kongruenten Zahlen bis zur Grenze von x hinzu und wendet als Exkludenten p = 13, 17, 19, 23 und 29 an, so schließen diese sämtliche Glieder von Ω mit Ausnahme von 197 aus. Dieses liefert in der Tat die Zerlegung:

$$18\,518\,809 = 197^2 + 1848 \cdot 100^2$$

M gibt sich somit als Primzahl kund, wie es schon von Euler festgestellt wurde (vgl. S. 57).

Da die Ausschließung einer Wurzel durch einen Exkludenten nach ihrem Reste bezüglich desselben sich richtet, dieser aber aus dem ihres positiv kleinsten Wertes durch Hinzunahme des entsprechenden Vielfachen des Modulrestes entsteht, so genügt die Kenntnis der positiv kleinsten Werte der Wurzeln.

2) $M = 34\,880\,077$.

34 880 077 ist $\equiv 5$ (mod. 8); ferner R3 N5 R7 N13. Die Zahl trägt mithin den Totalcharakter desjenigen Geschlechtes der Determinante $D_2 = -21\,840$, dessen reduzierte Formen

$$(37, \pm 8, 592)$$

sind (vgl. S. 127); ist sie prim, so erfährt sie durch dieses eine einmalige Zerlegung. Da das gleiche von 37 gilt, so wird somit

$$37 \cdot M = 37 \cdot 34\,880\,077 = 1\,290\,562\,849$$

durch die Hauptform (1, 0, 21 840) der Determinante $D_2 = -21\,840$ genau soviel Mal zerlegt als M durch (37, ±8, 592). Demnach gilt es, aller jener Zerlegungen oder aller positiven Lösungen der Gleichung

$$x^2 + 21\,840y^2 = 1\,290\,562\,849$$

habhaft zu werden. Zwei derselben charakterisieren M als zusammengesetzt.

Die Unbestimmte x, deren Wert von 0 bis $\sqrt{1\,290\,562\,849}$ oder von 0 bis 35 924 einschließlich schwankt, muß auf jeden Fall der Kongruenz genügen: $x^2 \equiv 1\,290\,562\,849$ (mod. 21 840); 1 290 562 849 ist $\equiv 1$ (3) $\equiv 4$ (5) $\equiv 2$ (7) $\equiv 4$ (13) $\equiv 1$ (16); somit $x \equiv \pm 1$ (3) $\equiv \pm 2$ (5) $\equiv \pm 3$ (7) $\equiv \pm 2$ (13) $\equiv \pm 1,7$ (16). Durch Kombination dieser Reste gehen als positiv kleinste Reste der Wurzeln hervor:

193, 353, 977, 1103, 1207, 1753, 2377, 2537, 2663, 3287, 3343, 3833, 3937, 4847, 4903, 5393, 5527, 6017, 6073, 6983, 7087, 7577, 7633, 8257, 8383, 8543, 9167, 9713, 9817, 9943, 10 567, 10 727, 11 113, 11 273, 11 897, 12 023, 12 127, 12 673, 13 297, 13 457, 13 583, 14 207, 14 263, 14 753, 14 857, 15 767, 15 823, 16 313, 16 447, 16 937, 16 993, 17 903, 18 007, 18 497, 18 553, 19 177, 19 303, 19 463, 20 087, 20 633, 20 737, 20 863, 21 487, 21 647.

Unter Anwendung der Exkludenten 11, 17, 19, 23, 29 und 31 fallen alle Glieder von Ω bis auf diese

193, 21 647, 22 033, 30 223

fort. Werden sie als Unbestimmte x in die Gl. $x^2 + 21840y^2 = M$ eingeführt, so verbinden sich nur 2, nämlich 21 647 und 22 033, mit Quadratwurzeln y. Sie geben die Zerlegungen:

$1290562849 = 21647^2 + 21840 \cdot 194^2 = 22033^2 + 21840 \cdot 192^2$.

Aus diesen folgen die Primteiler von M mit Hülfe des Verfahrens von S. 22. Der Bruch $\frac{21647 \pm 22033}{194 \pm 192}$ gibt:

1) $\frac{p_1}{q_1} = \frac{1}{1}$; daraus $\frac{ap_1^2}{cq_1^2} = \frac{1 \cdot 1^2}{21840 \cdot 1^2}$; $\frac{r_1}{s_1} = \frac{1}{21840}$;

$r_1 + s_1 = 21841$.

2) $\frac{p_2}{q_2} = \frac{193}{1}$; daraus $\frac{ap_2^2}{cq_2^2} = \frac{1 \cdot 193^2}{21840 \cdot 1^2}$; $\frac{r_2}{s_2} = \frac{193^2}{21840}$;

$r_2 + s_2 = 193^2 + 21840 = 59089 = 37 \cdot 1597$.

Damit sind als Primfaktoren von M gefunden: 1597 und 21841.

3) M = 14 687 329.

14 687 329 ist $\equiv 1$ (4) und R 3, N 7, N 29. Die prim angenommene Zahl wird mithin durch dasjenige Geschlecht der Determinante $D_4 = -2463$ zerlegt, dessen reduzierte Formen sind

(40, ±2, 61) (40, ±18, 69)

(vgl. S. 125). Da 40 durch jedes der beiden Paare entgegengesetzter Klassen nur einmalig zerlegt wird, stimmt die Zahl der Zerlegungen von 40 M durch (1, 0, 2436) oder von 20 M durch (2, 0, 1218) mit derjenigen von M durch jenes Geschlecht überein. 2 Zerlegungen von 20 M = 293 746 580 weisen somit M als zusammengesetzt aus und übermitteln gleichzeitig seine Faktoren. Gesucht sind also sämtliche positiven Auflösungen der Gleichung:

$$2x^2 + 1218y^2 = 293746580$$

Es ist erforderlich, daß die Unbestimmten x, deren Grenze $\sqrt{146873290}$ zu 12 119 angibt, der Kongruenz genügen

$2x^2 \equiv m'M$ (mod. 1218) oder $x^2 \equiv y$ (mod. 1218),

wo $2y \equiv m'M$ (mod. 1218). Die positiv kleinsten Lösungen der linearen Kongruenz sind 151 und 760; diejenigen der beiden quadratischen Kongruenzen $x^2 \equiv 151, 760$ (mod. 1 218)

37, 79, 443, 485, 733, 775, 1 139, 1 181

bzw. 124, 166, 530, 572, 646, 688, 1 052, 1 094

Die Exkludenten 11, 13, 17, 19 und 23 lassen im Kom-

plexe Ω nur die 5 Glieder zurück: 4 909, 6 011, 7 271, 8 692, 9 056, von denen allein das erste auf die Zerlegung führt:

$$2 \cdot 4\,909^2 + 1\,218 \cdot 449^2 = 293\,746\,580.$$

Mithin ist $M = 14\,687\,329$ prim.

4) $M = 308\,778\,563$.

308 778 563 ist $\equiv 3\ (8)$ und N 3, N 5, R 7, R 11, N 13.

Da M mithin den Totalcharakter desjenigen Geschlechts der Determinante $D_4 = -120\,120$ aufzeigt, dessen einfachste Formen sind:

$$(323, \pm 6, 372) \qquad (323, \pm 108, 408)$$

(vgl. S. 134), so ist dieses zur Zerlegung von M und damit die Hauptform (1, 0, 120 120) von D_4 zu derjenigen von 323 M in gleichem Maße befähigt. Sonach liegt ob, alle positiven Lösungen der unbestimmten Gleichung

$$x^2 + 120\,120\,y^2 = 99\,735\,475\,849$$

oder, da diese als Kongruenz nach dem Modul 120 120 übergeht in:

$$x^2 \equiv 99\,735\,475\,849 \pmod{120\,120}$$

die Wurzeln dieser Kongruenz aufzufinden.

Da $99\,735\,475\,849 \equiv 1\ (3) \equiv 4\ (5) \equiv 2\ (7) \equiv 9\ (11) \equiv 9\ (13) \equiv 1\ (8)$ ist, müssen die Wurzeln x gleichzeitig die Kongruenzen erfüllen: $x \equiv \pm 1\ (3) \equiv \pm 2\ (5) \equiv \pm 3\ (7) \pm 3\ (11) \equiv \pm 3\ (13) \equiv \pm 1, 3\ (8)$, wonach ihre positiv kleinsten Reste sich berechnen zu:

283, 1 537, 1 823, 2 467, 4 007, 4 183, 5 723, 5 827, 7 543, 8 473, 9 727, 10 007, 10 013, 11 833, 14 017, 14 297, 15 733, 16 013, 18 197, 20 017, 20 023, 20 303, 21 557, 22 487, 24 203, 24 307, 25 847, 26 023, 27 563, 28 207, 28 493, 29 747, 30 313, 31 567, 31 853, 32 497, 34 037, 34 213, 35 753, 35 857, 37 573, 38 503, 39 757, 40 037, 40 043, 41 863, 44 047, 44 327, 45 763, 46 043, 48 227, 50 053, 50 047, 50 333, 51 587, 52 517, 54 233, 54 337, 55 887, 56 053, 57 593, 58 237, 58 523, 59 777, 60 343, 61 597, 61 883, 62 527, 64 067, 64 243, 65 783, 65 887, 67 603, 68 533, 69 787, 70 067, 70 073, 71 893, 74 077, 74 357, 75 793, 76 073, 78 257, 80 077, 80 083, 80 363, 81 617, 82 547, 84 263, 84 367, 85 907, 86 083, 87 623, 88 267, 88 553, 89 807, 90 373, 91 627, 91 913, 92 557, 94 097, 94 273, 95 813, 95 917, 97 633, 98 563, 99 817, 100 097, 100 103, 101 923, 104 107,

104 387, 105 823, 106 103, 108 287, 110 107, 110 113, 110 393, 111 647, 112 577, 114 293, 114 397, 115 937, 116 113, 117 653, 118 297, 118 583, 119 837.

Der Bereich der Unbestimmten x reicht bis zu 315 809. Die Exkludenten 23, 29, 31, 37, 41, 43, 47 reduzieren den Komplex Ω auf folgende 6 Glieder:

30 313, 50 053, 118 583, 136 133, 198 377, 280 283.

Von diesen stellen nur das erste und vorletzte Lösungen x dar.

$$99\,735\,475\,849 = 30\,313^2 + 120\,120 \cdot 907^2 = 198\,377^2 + 120\,120 \cdot 709^2.$$

Die Primteiler von M liefert wiederum das Verfahren von S. 22.

Aus dem Bruche $\frac{30\,313 \pm 198\,377}{907 \pm 709}$ bildet man

1) $\frac{p_1}{q_1} = \frac{1155}{1}$; $\frac{ap_1^2}{cq_1^2} = \frac{1 \cdot 1155^2}{120\,120 \cdot 1^2}$; $\frac{r_1}{s_1} = \frac{1155}{104}$; $r_1 + s_1 = 1259$

2) $\frac{p_2}{q_2} = \frac{114\,345}{808}$; $\frac{ap_2^2}{cq_2^2} = \frac{1 \cdot 114\,345^2}{120\,120 \cdot 808^2}$; $\frac{r_2}{s_2} = \frac{3^5 \cdot 5 \cdot 7 \cdot 11^3}{8^3 \cdot 13 \cdot 101^2}$

$$r_2 + s_2 = 79\,218\,011 = 323 \cdot 245\,257$$

308 778 563 besteht also aus den beiden Primteilern 1 259 und 245 257; $308\,778\,563 = 1\,259 \cdot 245\,257$.

Die Ausschließungen erfolgten unter Zuhülfenahme der Gaußschen Exkludententafel für die Exkludenten 3, 5, 7, 11, 13, 17, 19, 23 (vgl. Gauß' Werke Bd. II, S. 508—509) und der Pepinschen für den Exkludenten 29 (vgl. Atti dell' Acc. Pont. Bd. 42 S. 146). Zu den größeren Primzahlexkludenten bestimmte der Verfasser dieser Arbeit selbst die ausgeschlossenen Linearformen für die einschlägigen Fälle der Rechnung, d. h. für den jedesmaligen Rest der Wurzel y der Kongruenz $\delta y \equiv m'M \left(\text{mod. } \frac{\Delta}{\delta}\right)$ bzgl. p.

Stellt man zum Schluß die Eulerschen und Gaußschen Methoden und ihre theoretischen Grundlagen einander gegenüber, so tritt die Überlegenheit der letzteren an ihrem gemeinsamen Berührungspunkte, nämlich der Benützung der 65 kongruenten Zahlen der Eulerschen oder der 65 einklassigen Determinanten D_1 der Gaußschen Formentheorie zur Primzahlbestimmung, zutage. Euler entdeckt seine numeri idonei

auf induktivem Wege; alle seine Bemühungen, seinen Satz über die kongruenten Formen theoretisch zu beweisen, schlagen fehl; zudem scheinen ihm die inkongruenten Formen vollkommen gleichwertig und an keine Gesetzmäßigkeit in der Darstellung der Zahlen gebunden. Gauß dagegen leitet die 65 D_1 deduktiv, aus dem Einteilungsprinzip des Formensystemes einer Determinante in Geschlechter und Klassen her. Er entkleidet sie dadurch ihres Charakters als Zahlenwunder und stellt sie als einen einzelnen Fall unter unzählig vielen andern dar, der in der Theorie sich durch nichts von diesen abhebt. Jenem Eulerschen Satz treten nun unzählig viele andere gleichartige an die Seite. Und welch ein Unterschied in den Methoden selber, zwischen dem Eulerschen Subtraktions- und dem Gaußschen Ausschließungsverfahren! Jenes läßt schon längst im Stich, während dieses noch verhältnismäßig rasch zum Ziele führt. Immerhin schiebt dieses die Grenze der untersuchungsfähigen Zahlen bloß hinaus, ohne sie gänzlich zu beseitigen, d. h. bislang fehlt noch ein praktisch brauchbares Mittel, über den primen oder zusammengesetzten Charakter jeder beliebigen, noch so großen Zahl zu entscheiden. Möge es die nahe Zukunft bringen und damit mehr Licht in das schon antike Primzahlproblem!

Lebenslauf.

Ich, Richard Burgwedel, wurde am 1. Juli 1884 zu Hagenau i. E. geboren. Nach dreijährigem Besuch der Volksschule zu Schiltigheim i. E. trat ich Herbst 1893 in die Sexta der Oberrealschule am Kaiserpalast zu Straßburg ein, welche ich Herbst 1902 mit dem Zeugnis der Reife verließ. Von Winter 1902 bis Sommer 1907 studierte ich Mathematik und Naturwissenschaften an der Kaiser-Wilhelms-Universität zu Straßburg und bestand Juli 1907 die Staatsprüfung für das höhere Lehramt. Von Herbst 1907 ab genügte ich meiner aktiven Militärpflicht und wurde nach Vollendung derselben am 1. Oktober 1908 als Probekandidat dem Lyceum zu Straßburg überwiesen. Nachdem ich anderthalb Jahre dieser Anstalt angehört hatte, wurde ich Ostern 1910 als wissenschaftlicher Hülfslehrer an das Gymnasium in Weißenburg versetzt.

Allen meinen akademischen Lehrern danke ich bei dieser Gelegenheit für die von ihrer Seite mir zuteil gewordene Ausbildung und Förderung, in erster Linie Herrn Prof. Dr. Weber, der mir die Anregung zu vorstehender Arbeit gegeben und mir in jeder Weise sein Interesse für dieselbe bekundet hat.

G.E. STECHERT
& Co.
NEW YORK

UNIVERSITY OF ILLINOIS-URBANA
512.73B91U C001
UBER DIE EULERSCHEN UND GAUSSSCHEN METHO
3 0112 017074292